“ La blockchain au regard du droit et de l’identité ”

Thibault Langlois-Berthelot

École des Hautes Études en Sciences Sociales

EHESS doctoral school

Georg Simmel Center

Doctorate in

LAW AND SOCIAL SCIENCES

THIBAULT LANGLOIS-BERTHELOT

BLOCKCHAIN IN THE CONTEXT OF LAW AND IDENTITY

Thesis directed by : MR. RAINER MARIA KIESOW

Date of defense : June 15, 2023

Rapporteurs
1 MRS CAROLINE LEQUESNE-ROTH
2 MR. GRÉGOIRE LOISEAU

Jury

1 MRS VALÉRIE CHAROLLES, STATUTORY RESEARCHER, HDR, POLITICAL ANTHROPOLOGY LABORATORY CNRS/EHESS

2 MR. RAINER MARIA KIESOW, DIRECTOR OF STUDIES, EHESS

3 MR. JEAN LASSÈGUE, DIRECTOR OF RESEARCH, CNRS

4 MRS CAROLINE LEQUESNE-ROTH, SENIOR LECTURER, HDR, CÔTE D'AZUR UNIVERSITY

5 MR. GRÉGOIRE LOISEAU, PROFESSOR AT PARIS 1 PANTHÉON-SORBONNE UNIVERSITY

To all my family and friends, past and present.

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to all the people who made this thesis possible. I would like to thank my thesis supervisor for his constant support and trust. I would also like to thank my colleagues at IN Groupe who have supported me, and my friends who have given me moral comfort and invaluable help throughout my academic career. This thesis has been enriched by numerous interventions and hearings, notably at public meetings, private discussions, colloquia and various other events. I would like to thank the many academic and/or professional participants. Finally, I would like to thank my family for their unfailing support throughout my research.

SUMMARY AND KEYWORDS

For over a decade, blockchain technologies have been progressively and profoundly redefining the political, legal and economic boundaries of our social contract. Some of its features liberate as much as they challenge the established order, i.e. existing models of governance. In collaboration with IN Groupe, this interdisciplinary study examines how the positioning and prospects of these new technologies relate to, oppose or fit into current legal and social frameworks. For several decades now, the concept of digital identity has been constantly evolving and being interrogated by the sciences in response to the meteoric expansion of people's online interactions and identification needs. This insatiable digitization of our lives implies new philosophical, social and legal considerations in light of the many facets of our identities, which are already 'phygital'. Alongside these attempts to define and reappropriate identity scientifically, we also suggest concrete, up-to-date ways of thinking about the emergence of a new digital identity 3.0. Assumed to be decentralized, emancipatory and at the service of digital rights, we identify how decentralized digital identity and blockchain technologies represent a revolution in search of new rules of law. By taking a snapshot of socio-digital (eco)systems, this study examines the consequences of these new Web 3.0 decentralization technologies, enabling individuals to hold universal digital proof of existence in line with their fundamental rights, which are now cryptographic and programmable. A preferred line of thinking also suggests that certain open, decentralized blockchains should not be prohibited or discredited, in order to satisfy the ongoing needs of Internet users and citizens for trust and cryptographic ownership. These infrastructures can indeed serve as a digital alternative and counter-power, particularly in developing countries.

Key words

Legal sciences, computer sciences, decentralization, Bitcoin, blockchain, crypto-assets, decentralized digital identity, Web 3.0

ABSTRACT AND KEY WORDS

For more than a decade, blockchain technologies have been gradually and deeply redefining the political, legal, and economic boundaries of our social contract. Some of their characteristics both liberate and challenge the established order, i.e. existing governance models. In collaboration with the IN Groupe company and through an interdisciplinary lens, this paper examines how the positioning and perspectives of these new technologies are articulated, opposed, or integrated into current legal and social frameworks. In parallel with societal upheavals analyzed in the context of computer decentralization, the concept of digital identity has been evolving and questioned for several decades to cope with the explosive expansion of online interactions and identification needs of individuals. This insatiable digitization of our lives implies new philosophical, social, and legal considerations considering the many facets of our already 'phygital' identities. These attempts at defining and scientifically reclaiming identity also evoke new concrete lines of reflection regarding the emergence of a new digital identity 3.0. Supposedly decentralized, emancipatory, and serving digital rights, we identify how decentralized digital identity and blockchain technologies represent a revolution in search of new legal rules. By examining socio-digital (eco)systems, this study questions the consequences of these new Web 3.0 decentralization technologies, allowing individuals to hold universal proof of digital existence in line with their fundamental cryptographic and programmable rights. A privileged line of reflection suggests that it is crucial not to prohibit or discredit certain open and decentralized blockchains, to satisfy the continuous needs of trust and cryptographic ownership of Internet users and citizens. These infrastructures can indeed serve as an alternative and digital counterbalance, particularly in developing countries.

Keywords

Legal sciences, computer sciences, decentralization, Bitcoin, blockchain, crypto-assets, decentralized digital identity, Web 3.0

Warning

Neither the École des Hautes Études en Sciences Sociales nor IN Groupe intend to give any approval or disapproval to the opinions expressed in this thesis.
These opinions must be considered as the author's own.

Contents

Table of contents

Introduction

Any social construction requires the implementation of identification mechanisms, so that each person can effectively recognize him or herself, i.e. identify with him or herself. This need for identification is explained by the individual and collective attribution of rights and duties in order to form a society. From its most primitive forms, such as the attribution of a customary name based on physical appearance, to today's unique and accomplished forms of identification, such as biometrics coupled with the use of identity documents with digital capabilities, the forms of expression of identity are multiplying and intersecting in the digital age. Today, more than ever, identity is a polysemous concept that can be defined from philosophical, social and legal angles, in order to capture the lived identity of individuals, i.e. both the contexts and the identification needs with which they are confronted on a daily basis. Identity is made up of several contexts: a temporal context, a social context and a territorial context. Whether offline or online, identity is thus a mise en abîme of which we master only certain components, while having the impression and intuition of possessing a perfect understanding. For example, an identity card carries and fixes certain legal characteristics of a person, while at the same time considering that they remain relative over a long period of time, as they change with each person's social history. One of the aims of this study is to raise awareness of digital identity in general, so that every individual is aware of the emergence of a digital quintessence, i.e. a more open, transparent and decentralized third-generation Internet, Web 3.0.

All interconnected and dematerialized, social interactions are constantly optimized to meet the needs of individuals, with digital technology representing a third industrial revolution[1] . Ever more global, rapid and personalized, today's communications mark a civilizational shift from *homo sapiens* to *homo numericus*[2] . In less than half a century, this profound (r)evolution has become the source of planetary societal progress. Our ability to exchange all kinds of information, leading to all kinds of interactions, has been multiplied thanks to social networks and digital platforms (Uber, Google Maps, remote meetings) whose pioneering infrastructure remains the Internet. By 2021, almost 5 billion people with an Internet connection can enjoy the benefits of being connected to the rest of the world[3] . Today, many online interactions require a digital identity to join communities, access services and gather information, publish ideas or manage finances online. In its early days, the Internet was not structurally designed to provide all its users with a digital identity, which explains today's multiple identification and authentication solutions.

[1] ROUTLEY Nick, "The multi-billion dollar industry that makes its living from your data," March 10, 2019, available online.
[2] COMPIEGNE Isabelle, "La société numérique en question(s)", chap. V, Qui est l'homo numericus? pp.59-70, Éd. Sciences Humaines, 2010.
[3] PETROSYAN Ani, "Number of internet and social media users worldwide as of January 2023", in *Statista Inc,* online

that each individual tries to appropriate. In response to this need to identify Internet users, each online service offers a more or less reliable and data-intensive form of digital identification. This massive delegation of digital identities has led to a lack of digital trust, notably due to the structural dependence of users on these online services. For example, while it's easy to digitize information today, it's more complex to trust it once it's in circulation in the digital world, for example with regard to its integrity, validity or origin. Faced with the growing scale of these phenomena, which regularly generate infringements of people's rights, legislators are attempting, with varying degrees of harmonization and success, to regulate this digital sphere. The Internet may be virtual, but its consequences are very real for Internet users. The world of information technology is neither separate from nor ancillary to the physical world, but complements it and is gradually becoming essential to the social pact.

A formidable tool for economic and social prosperity and freedom for some, a slow drift towards technocracy[4] by misappropriation of purpose for others, the Internet undoubtedly represents a socio-technical revolution that is as unprecedented as it is half-hearted[5] . Indeed, the exponential growth and use[6] of the digital universe is reaching a climax with the virtual confinement of Internet users to their online services, whose design all too often helps to introduce a form of psychosocial dependency. As a result, the subjective identity constructed and asserted online tends to grow in importance in such a way that the digital universe has never been so aptly named. However, this tremendous progress in digital communications must be seen in the context of the computerized and legal dispossession it entails for people's *phygital* identity[7] , who find themselves over-personalized, or even deprived of certain rights and elements of their identity (manipulation of public opinion, rumors, harassment). In 2022, it was reported that more than a billion customers or citizens had suffered data theft[8] . According to a study published the same year, the majority of Americans feel they have little control over the data collected by companies and the government about them[9] . These observations are shared throughout the world, and demonstrate the initial limits of this digital sphere, which is sometimes more idyllic than it actually is. The dystopia of Web 2.0 should not, however, overshadow the potential of other technologies.

[4] Wikipedia, the free encyclopedia, *Technocracy*, March 30, 2022, available at
[5] "Le numérique se présente ainsi tout à la fois comme témoin, catalyseur et source des bouleversements du droit", in *Annales des mines* n°18 and in *Propriété et gouvernance du numérique*, Institut Mines-Télécom, June 2022, p.9.
[6] REINSEL D., RYDNING J., GANTZ JF., "The world keeps creating more data - now, what do we do with it all". See also: "The amount of digital data created over the next five years will be more than twice the amount of data created since the advent of digital storage", in *Worldwide global data sphere forecast 2021-2025,* accessed March 20, 2021 at
[7] Wikipedia, the free encyclopedia, *Phygital* is a contraction of the words '*physical*' and '*digital*'.
[8] Forrester reveals lessons learned from Top 2022 data breaches. In *Forester Media*, February 24, 2023, available at
[9] AUXIER Brooke et al, "Americans and privacy: concerned, confused and feeling lack of control over their personal information," in *Pew Research Center*, November 15, 2019, available at.

of Web 3.0 at the service of people's psychosocial and legal identity, i.e. at the service of a safer Internet.

The *phygital* evolution of our social interactions is concretely possible thanks to multiple successive and interwoven technological revolutions. From the Internet and conventional computing 1.0 through digital identity 2.0, to the recent verifiable computer standards or blockchain infrastructures[10] decentralized and 3.0, our research studies the transversal impacts of each of these technologies on identity as well as on people's rights, founding notions of any social contract. Other more disruptive, but still uncertain, technologies, such as genetic digital identity 4.0 and quantum computers 5.0, are also analyzed in an attempt to project this study into the long term. For more than a decade, a new technology has been revolutionizing our relationship with online interactions and monetary transactions: the Bitcoin blockchain. This recent blockchain technology, which initially underlay bitcoin (with a small b throughout our research), has become the source of numerous caricatures of all kinds, i.e. as many fantasies as fears concerning its functioning, its legal and societal impacts or even its business use cases. Later, it gave rise to many other technological forms of blockchain, with varying degrees of decentralized computing. In 2021, the global market for blockchain technologies was valued at $4.7 billion, and could reach $164 billion by 2029[11] . The crypto-asset sector using blockchain technology could reach one billion users by 2030, according to a report published in 2022 by the Boston Consulting Group (BCG)[12] . For the record, 1998 was a similar period when commercial companies such as Google, PayPal and Netflix were created. In parallel with these blockchain technologies, decentralized digital identity (IND) embodies the idea of an online identity that is independent of a central authority or third party in order to be computerized and valid. It can be linked to blockchain technology to store and manage identity data in a decentralized way, i.e. without the need for a central authority such as public institutions or corporations to administer and control it. This conceptual and technological paradigm shift for digital identity offers new transparency, accessibility and social and digital openness for Internet users and online identity and service providers. When a decentralized identity uses an open blockchain, this association

[10] The term is used in the plural throughout this study to emphasize the multiple aspects and IT variants of this technology.
[11] "Blockchain market size, share and Covid-19 impact analysis, forecast 2022-2029", in *Fortune business insights*, March 2022 available at.
[12] "What does the future hold for crypto exchanges?" in *Boston Consulting Group*, July 2022, available at p.10.

between a decentralized electronic registry and the verifiable identity data it hosts, offers a universal digital identity for the first time[13] .

For author and mathematics doctor Aurélie Jean, new digital technologies are often misunderstood by the general public, "*whereas we should all be enlightened and integrated inhabitants of the land of algorithms, we are merely ill-informed tourists, with no real access or map to understand its reliefs and secrets*"[14] . Blockchain technologies represent a complex digital mutation to which the law must adapt, as there are as many blockchains and their underlying technological bricks as there are multiple possible organizational variants. Because their governance, strength and legal framework are currently uneven. We will discuss how smart contracts and other applications of blockchain technologies will change the nature of digital interactions between individuals. For example, since around 2015, anyone with an internet connection can use crypto-assets with multiple and varied purposes and operations without permission. The Bitcoin blockchain (here with a capital B to designate this technology) has initiated a movement to open up and issue private (crypto)currencies, i.e. legally unrecognized by states, which has gradually given rise to multiple underlying applications such as autonomous organizations and decentralized social networks, the majority of which to this day run in complete ignorance of legal frameworks. These applications and programs have already produced new social and legal effects, expressed by a "*lex cryptographia*" as early as 2015[15] , following the example of a *lex mercatoria* or *lex electronica*.

At the same time, identity today seems as complex to define[16] as it is to protect and implement in the digital space. The law limits its definition to certain material elements, whereas identity now seems to be a multi-dimensional concept for the digital sphere, i.e. a static legal identity in civil status versus a fluid online digital identity. Uncertain geopolitical contexts are likely to accentuate the use of these technologies.

3.0 in data security and traceability, always involving the digital identity of a person and a machine. This study deals with the legal and digital identity of individuals, i.e. limited to the transactions and interactions that make it strictly necessary. It is analyzed in terms of

[13] PERSON Pierre, jurist and former MP, "L'universalité et l'ouverture, fondements même de la blockchain : vers une nouvelle ère crypto, un enjeu de souveraineté et de compétitivité économique, financière et Monétaire", in *Rapport de l'Assemblée Nationale, quinzième législature, 2022*, p.182.

[14] JEAN Aurélie, "Les algorithmes font-ils la loi?", online version in *decitre.fr*, Humensis, 2021, reading position in book: 22%.

[15] WRIGHT Aaron, De FILIPPI Primavera, "Decentralized blockchain technology and the rise of Lex Cryptographia", March 25, 2015, online at ; MIRANDA Maxime, "vers le développement d'une Lex Cryptographia", November 13, 2017, in *Droitdu.net*.

[16] MAALOUF Amin, "A lifetime of writing has taught me to be wary of words. Those that seem clearest are often the most treacherous. One of these false friends is precisely 'identity'", in *Les identités meurtrières*, 2021, p.15.

In other words, through the prism of its purposes, contexts of use and use cases. As a matter of principle, legal experts use the law to apprehend a new technology, looking for the different ways in which it might be used, but sometimes straying from the IT qualification of technologies, i.e. their IT understanding. It is proposed that the reading be reversed, i.e. to study certain new technologies and then their applicable rules, in order to carry out a legal analysis as close as possible to what exists digitally. It is also proposed to use the scientific literature on these new 3.0 technologies to take a transversal look at several years of events within the Internet 3.0 ecosystem.

Analysis of the scientific literature on digital identity shows growing Internet searches related to these terms from 2004 to the present[17] and a significant rise in interest in the concept of identity from the 1800s to 2014[18] , with a similar finding for blockchain technologies from 2010 to 2019[19] . At the beginning of 2023, French case law on identity numbered 122,822 court and tribunal decisions, almost exclusively based on the notion of identity control[20] . In the same period, 338 companies were registered with the Registres des Commerces et des Sociétés (RCS) of the commercial courts with the term blockchain in their corporate purpose[21] . This figure is relatively large compared to the presumed 716 companies operating in the blockchain technology market and officially listed in the EU in 2022[22] . Worldwide, 1,286 projects have been identified, the majority of which are located in Europe and the USA[23] . A graphical analysis of the sectoral use cases and applications of this panel shows that 20% of these projects relate to the monetary and financial sector, while 10% to the property and digital identity sector. As far as Bitcoin's blockchain infrastructure is concerned, academic literature shows that there are approximately 22 doctoral theses in law available online in France that mention this technology[24] . Of these, more than 50% mention the Bitcoin protocol (capitalized) or its native token bitcoin (lower-case) in a negative or at best relatively neutral light (only 3 out of 22 theses adopt a neutral perception). This negative discernment materializes in references to its supposedly intrinsically dedicated use for money laundering, terrorist financing or elite corruption. Conversely,

[17] Concerning Internet searches related to the term "digital identity" see the curve on *Google Trend at the* following address; *Id.*, for the term "blockchain" see the following curve.
[18] "Google Books Ngram Viewer", graphic presenting the term "identity" mentioned in literary works from 1800 to 2019, online at
[19] "Google Books Ngram Viewer," graph showing the term "blockchain" mentioned in literary works from 2010 through 2019, online at.
[20] V. Justice.pappers.fr, search for court decisions, available online
[21] *Ibid,* Company search, available at
[22] Directory of European Blockchain Startups, August 23, 2022, *ChainEurope*, available at.
[23] Data analysis and charts from the Blockchains and Sustainable Development Observatory, "Blockchains and Sustainable Development Observatory", February 23, 2023, available at Association Blockchain for Good
[24] Retrieved from Theses.fr online on April 04, 2023. Although 42 theses are listed on this subject, only 22 are accessible online, allowing a brief analysis of their content relating to the Bitcoin blockchain

only a minority (32%, i.e. 7 out of 22 theses) adopt a positive perception, that of an open digital infrastructure offering a relatively viable alternative currency.

In Europe, France is a pioneer behind Switzerland when it comes to the legal framework for crypto-assets, albeit with nuanced economic and social consequences. At Community level, a cross-border legal framework applicable within the EU is in the process of being adopted (studied below) and will influence many jurisdictions in the years to come. Some of them are planning to regulate these new technologies, while international legal harmonization remains in its infancy[25] . While the legal framework for crypto-assets appears to be more advanced in Europe, there does seem to be a political motivation to slow down the adoption of the open, public blockchain technologies on which they are based. This is due to a desire to promote more closed and controllable versions of the technology, in other words, to favor the deployment of so-called private or hybrid blockchain technologies (which do not incorporate crypto-assets). Political powers oscillate variably between rhetoric aimed at attracting crypto-economy players, while regulations intensify to the point of sometimes jeopardizing the most fragile players in these 3.0 ecosystems. By way of illustration, a report published in 2022 by the Direction Générale des Entreprises (DGE)[26] stresses the alleged advantages of closed blockchain technologies over public blockchain technologies, which are said to consume too much energy or be computationally inefficient.

To date, academic research has focused more on the notion of crypto-assets or the governance of decentralized systems. The aim is to define why and to what extent the modes of governance of decentralized digital identity systems differ from the centralized alternatives still in use. A lack of political awareness seems to persist both for certain blockchain technologies and for the concept of decentralized digital identity (IND), a notion that is relatively unknown due to little research in France on the subject[27] . According to a study published in October 2021[28] , France is the 6th[e] out of 33 countries to have published at least one scientific paper on the subject of decentralized digital identity, representing just 6.7% of all publications. However, interest in this new field of research seems to be growing: "*if we consider overall growth, from 2017 to 2021, the number of articles* [on IND] *increased by 96.7 %*"[29] . As mentioned above, some public institutions issue civil and political identity cards.

[25] PERSON Pierre, "La réglementation des cryptoactifs vit ses balbutiements. [...] the beginnings of this future regulation are extremely disparate", *op. cit.* p.12.
[26] V. Blockchain Awareness Guide | entreprises.gouv.fr., April 13, 2022, www.entreprises.gouv.fr
[27] Only 3,332 documents in French containing the terms "identité décentralisée" are referenced on Academia.edu, compared with 152,015 found in English, in Academia.edu | Search | identité décentralisée, searches performed online on November 18, 2021.
[28] CUCKO Spela, TURKANOVIC Muhamed, "Decentralized and self-sovereign identity: systematic mapping study", October 15, 2021, *Faculty of Electrical Engineering and Computer Science*, University of Maribor, Slovenia, p.10, available online
[29] *Ibid.* p.9.

At the same time, they face the challenge of digitizing social interactions. This raises the question of how to continue to ensure the exercise and protection of people's identities and rights in the digital age, from the State to "*Big Data*"[30] . To illustrate this point, institutions such as IN Groupe (ex-Imprimerie Nationale)[31] have been offering to materialize people's civil identities on trusted physical media (CNIe, passports) for over 500 years. However, the rise of digital technologies and behaviors has led to a redefinition of this institution's positioning from the physical and regal identity market to the *phygital* and sometimes exclusively digital market. This strategic and technological transition, successfully initiated by the institution, could lead to digital technology replacing the need for physical identity documents within several decades. Such an eventuality would have irreversible consequences, which need to be weighed up against the risk of technological aberrations, such as the digital suppression of online identities. It is therefore essential to consider 3.0 technologies as a guarantee of a person's digital identity. It is all the more necessary to recreate trust at a time of widespread data sharing and the multiplication of online services. For example, by accepting the general terms and conditions of use, each citizen can create numerous accounts in just a few clicks, whose effective and definitive deletion of data can take several months. While it is legitimate to consider that major technology companies are pursuing their commercial aims, they must more than ever respect the legal and regulatory framework of their activities in order to avoid abuses as demonstrated by the famous Snowden cases in 2013[32] and Cambridge Analytica in 2018[33] . As applications and large companies have become de facto identity controllers, users have progressively lost control over their digital data and identities and thus increased their IT and social dependency. Decentralized identity could therefore represent a counterweight to the centralization of identity data and its excesses. The digital society now undergoing a far-reaching revolution with the adoption of new blockchain technologies and the emergence of decentralized digital identity seems to raise at least three major questions:

(i) Is IT and social decentralization necessary, utopian or beneficial for a new digital trust? Are 3.0 technologies incompatible with the rule of law?

[30] 'Metadata' or 'massive data', providing important information about our habits, behavior, tasks, etc.
[31] Became Imprimerie Nationale SA under law no. 93-1419 of December 31, 1993, amended by implementing decree no. 2006-1436 of November 24, 2006, available at the following address
[32] Wikipedia, the free encyclopedia. "Snowden" (film), consulted on June 26, 2022 at the following address
[33] Facebook subsidiary Cambridge Analytica (now *Meta*) contributed in 2016 to the election campaign of US President Donald Trump - as well as that of Boris Johnson in England - due to the harvesting, analysis and then influence of user data from the Facebook and Instagram social networks. To illustrate, this company had over 5,000 data points relating to every American voter. Psychologist and doctor Michal Kosinski proved that from a minimum of 68 "likes" on Facebook, it is possible to predict a person's skin color (95% effective), sexual orientation (88%) and political beliefs (85%). Wikipedia contributors, the free encyclopedia, March 17, 2023, available online

(ii) Do blockchain technologies and decentralized identity characterize a 3.0 revolution for people's psychosocial and legal identity?

(iii) Will Internet users prefer a decentralized IT infrastructure that is resilient but monofunctional and not legally compliant, or a centralized infrastructure with multiple functionalities that is legally compliant but not resilient?

It's safe to assume that 3.0 technologies will enable us to move away from a form of wild digital identity towards a digital identity gradually controlled by Internet users. However, to qualify this degree of control, which in reality varies according to the online context, we must remember that behind any machine or computer protocol there remains the hand of Man. This raises the question of whether it is appropriate to create a specific law for the phenomena of computer decentralization. For over a decade now, Internet users have been able to create and share value peer-to-peer on the Internet thanks to blockchain technologies, without relying on third parties (banks, computer servers). Should legislators encourage or curb this liberalization of online identity, now exacerbated by the possibility of pseudo-anonymity (developed further below) and disintermediation of exchanges? Is the advent of a new cryptographic law 3.0 necessary and viable? Our hypothesis is that blockchain and digital identity technologies can at best make people's online rights more democratic by strengthening their freedoms. In this way, the present research will lead us to understand the urgency of implementing more decentralized IT solutions to enable the advent of a genuine cryptographic right. This research studies the extent to which a partial decentralization of primary digital identity is necessary, and whether a total decentralization of secondary digital identity is desirable. It is also proposed that the two digital identity schemes, one centralized and the other decentralized, should not be pitted against each other, but should be conceived as complementary and hybrid[34] . Decentralized identity is an opportunity of general interest that will make it possible to provide a single identity for all digital ecosystems and online services (abolition of multiple usernames and passwords), more fluid and personalized payments (possibly coupled with crypto-assets), more secure messaging and communications that respect privacy (decentralized social networks), in other words a more secure, neutral Internet that respects people.

We will determine the potential of existing blockchain technologies, which will be relaunched as new technologies are adopted, the European Commission having declared itself in favor of a harmonized and partially decentralized European digital identity "*an electronic identity*".

[34] A hybrid digital identity refers to a digital identity derived from both Web 2.0 and Web 3.0. It comes from the former, as it is often derived from a physical identity materialized by a credential. It also stems from the latter, thanks to the decentralized identity standards enshrined in this thesis. In other words, in IT terms, a *hybrid digital identity* is partially decentralized, i.e. *semi-decentralized* or conversely *semi-centralized.* V. Glossary.

universally accepted public ID (eID) is needed so that consumers can access their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily share personal data with them."[35] . We will also determine how these 3.0 technologies will provide universal proof of existence in line with people's rights and identity. We will start from the assumption that a legal framework should be necessary for certain 3.0 solutions, particularly in the financial and monetary fields, but that a legal intervention understood as tailored and proportionate should nevertheless tolerate the decentralized monetary experimentation represented by the oldest blockchain technology, Bitcoin. While regulation must ensure the dissemination of certain legal guarantees for its users, the Bitcoin blockchain already provides them with computerized confidence. Decision-makers and legislators must take care to design coherent legal rules that are as close as possible to society's socio-technological needs and experiences.

"Europe must now take the lead in adopting and standardizing the new generation of technologies: blockchain, supercomputers, quantum technologies, algorithms and tools for sharing and using data"[36] . Each new technology represents a new tool and support in the service of Man and his values, and Web 3.0 is no more than a new medium and vector of communication[37] , as paper has been for centuries. French philosopher Bernard Stiegler points out that "*every technical object is pharmacological: it is both poison and remedy. The pharmakon is both what enables us to take care of and what we have to take care of, in the sense that we have to be careful with it: it is a curative power in the measure and disproportion in which it is a destructive power*"[38] . By analogy, any new computer technology, whatever its medium or content, can be manipulated, misinformed or a source of inequality[39] . While new 3.0 technologies are not immune to this reality, they are able to avoid it by providing evidence of reliability and trust. One thing is certain: any new technology often takes longer than it seems to mature and achieve satisfactory social adoption.

In the light of these introductory remarks, which will be backed up by field experiments carried out at IN Groupe (formerly Imprimerie Nationale), and in the French Web 3.0 ecosystem since 2020, we propose in the first part to study the epistemology of identity and of

---

[35] Free translation from English. "Communication Shaping Europes Digital Future", accessed online December 6, 2021, p.6.
[36] *Ibid*, p.7.
[37] JEAN Aurélie, "Les algorithmes font-ils la loi?", "The algorithm is not guilty for the simple reason that it is neither a physical nor a moral person, and that it is men and women who decide on its use, implementation and resulting effects, and who are therefore solely responsible", *op. cit*. in *Humensis*, 2021, reading position in the book: 19%.
[38] STIEGLER Bernard, "Questions de pharmacologie générale. Il n'y a pas de simple pharmakon" in *Psychotropes,* 2007/3- 4, Vol. 13, pp.27-54, available at
[39] MAZEREEUW Faustine, "Le numérique est une gigantesque machine à renforcer les inégalités", in *Les Echos Start*, published February 17, 2023, interview by Mathilde Saliou, digital journalist at Next Inpact.

blockchain technologies through the prism of philosophy, social sciences and computer science (**Part I**, **Title 1**, chapters 1 and 2). We will examine the balance that exists between law's quest for stability and the constant technological and social mutations it faces, in support of the promises and challenges of the digital 2.0 society and a transition to decentralizing and emancipating 3.0 technologies (**Title 2**, chaps. 1 and 2). In the second part, we introduce the concept and its societal stakes of a decentralized digital identity at the service of the universality of people's rights (**Part II**, **Title 1**, chapters 1 and 2), before analyzing several use cases and transversal and specific projects, some of which have already been deployed in favor of the adoption of a 3.0 digital identity (**Title 2**, chapters 1 and 2).

I/ Epistemology of legal identity and blockchain technology

Title 1: The complex, ductile perimeter of identity

Chapter 1: Identity as a complex philosophical, social and legal object

1.1 Defining the fields of identity and its mechanisms

The aim of this first part is to explore the different meanings of the notion of identity. The aim is to assess the various possible definitions that have been attributed to it in the course of the evolution of society, which is now subject to progressive digitization. A transversal analysis of identity is required, from its philosophical and social apprehension to its digital and legal definition. Over the past few decades, the concept of identity has been increasingly evoked by a variety of disciplines, including computer science, politics, social studies and law. These disciplines are unanimous on the difficulty of apprehending and defining the concept of identity. In other words, there is no truth to a general definition that would satisfy all the sciences. There are as many definitions of the notion of identity as there are authors writing on the subject, due to the many different situations, with meanings as different as they are contradictory. In the same way as a technology, identity could only be a social tool at the service of individual and collective social perception and attribution. To explore the contours and different meanings of this seemingly elusive definition, this section considers the term identity through its multiple facets, which are presented in a non-limitative way in the table below, according to our research and understanding.

:

Total number of equivalents found in the literature	**Type of vocabulary associated with the term "identity" from scientific literature**	**Category 1:** ***Philosophical identity***	**Category 2:** ***Social identity***	**Category 3:** ***Legal identity***
1	*Lived identity*	X	X	
2	*Moral identity*	X	X	
3	*Subjective identity*	X	X	
4	*Psychological identity*	X	X	
5	*Perceived identity*	X	X	
6	*Claimed identity*	X	X	
7	*Elementary identity*		X	X
8	*Legal identity*			X
9	*Civil and legal identity*			X

10	*Extended identity*	X	X	X
11	*Root identity*			X
12	*Biological identity*	X	X	
13	*Genetic identity*	X	X	X
14	*Plural identity*	X	X	
15	*Singular identity*	X	X	X
16	*Relative identity*	X	X	
17	*Contextual identity*	X	X	
18	*Social identity*		X	X
19	*Collective identity*		X	X
20	*Temporal identity*	X		
21	*Body identity*		X	X
22	*Cultural identity*	X	X	X
23	*Etymological identity*	X	X	
24	*Anthropological identity*	X	X	X
25	*Gender identity*	X	X	X
26	*Siloed identity*	X	X	
27	*Identity in context*	X	X	
28	*A shared identity*	X	X	X
29	*Murderous identity(ies)*	X		
30	*Negotiated identity*	X	X	
31	*Narrative identity*	X	X	
32	*Generic identity*		X	X
33	*Specific identity*	X	X	X
34	*Identity of choice*	X	X	
35	*Administrative identity*			X
36	*Derived identity*	X	X	
37	*Pivotal identity*			X
38	*Regalian identity*			X
39	*Primary identity*			X
40	*Secondary identity*	X	X	

Total	**~ 40 occurrences regularly cited in scientific literature**	**28**	**31**	**20**

The analysis of this prospective table allows us to hypothesize that identity is mostly recognized in scientific literature through philosophical, social and legal acceptance. This rapid comparison also enables us to group together adjectives and terms that refer to close or similar concepts of identity. It is generally accepted that the identity of a person, organization or thing refers to everything that is likely to characterize them. In a general sense, for individuals, identity encompasses both their physical (biometric) characteristics[40] and other characteristics such as their social interactions, experiences, titles or possessions. As a result, there are an infinite number of attributes that make up our identities as human beings, most of which are constantly evolving, which explains the ductile nature of identity. Given the sheer quantity of attributes and factors that contribute to a person's identity, it becomes complex to organize them, i.e. to collect, store and index them within a single physical or digital space. For this, the use of trusted actors - designated as trusted third parties (companies, state institutions) - has historically been necessary to provide people with a stable, trusted identity, with the latter ensuring centralized management and distribution of their identity attributes. Academic and literary definitions of the notion of identity reflect its multidimensional aspect. According to the Académie Française online dictionary, the term "identity" has four possible meanings. The first refers to an "*exact resemblance between beings (...) who have a distinct existence*", thus referring to identity in the physical sense of the term. The second refers to a more abstract and relative identity, an identity of nature, "the *character of that which is one or constitutes one and the same reality* (...)". The third refers to a psychosocial identity, i.e., to what "*forms the basis of individuality"*. Finally, the last definition refers to a legal identity, i.e. "the *civil personality of an individual, legally recognized or established by various elements of civil status (...)*". More generally, the encyclopedia defines identity as "the *permanent and fundamental character of someone, of a group, that makes up its individuality, its singularity*"[41] , this term being derived from the Latin "*idem"* meaning "*the same, the same, the same thing"* when used as an adjective or pronoun. This literal Latin translation of the term identity is attributed to the work of reflection and translation carried out by the French philosopher Paul Ricœur in his book "*soi-même comme un autre*"[42] . It would appear that no single scientific discipline tackles this question on its own.

[40] V. Title II, chap. 1, 1.3
[41] Larousse Éditions, "Identité" (Low Latin identitas, -atis, from Classical Latin idem, the same), accessed online on August 18, 2021.
[42] RICOEUR Paul, "soi-même comme un autre", accessed August 18, 2021, ISBN 2-02-011458-5, available at

identity, in an attempt to give it a precise and universal definition. To define identity, we need to look at it from a number of different angles, sometimes complementary, sometimes incompatible. Although the notion of identity is present in many social science corpuses and reflections, it remains highly plurivocal and enigmatic. Identity is a good way of proposing a multi-disciplinary analysis, not of the reality it describes, but of its multiple realities and contexts of use. A number of questions can be raised: for example, is it illusory to try to define identity? Is there such a thing as one or several identities? To what extent do the uses of identity allow us to define its contours? What assimilation or confusion exists between physical identity, social identity and legal identity? Does the dematerialization of a physical identity affect its integrity or just its substance?

Identity can be seen as a multifaceted concept, from which each science draws its own conclusions[43] , enabling us to understand it in both a global and multidisciplinary way. The role of the sciences is to propose a fairly general and impersonal identification of people on an individual scale. So, depending on the science involved, the notion of identity will not have the same meaning or scope. For example, psychology refers to personal identity, sociology to group identity and law to legal identity. This polysemous essence of the term identity calls for a multitude of contexts and situations that need to be studied with care, to avoid resorting to a systematic generalization of the concept of identity. However, it seems that a degree of generality is necessary, so that anyone can understand what we are talking about in terms of the two approaches generally accepted in the physical and digital worlds:

(i) A first approach assumes that each person has a unique identity. All data generated by an individual can be attributed to that person, either directly or indirectly. According to this approach, each piece of data is unique because it represents one or more aspects of the uniqueness of its owner's identity. Such a definition assumes that the identity is unalterable over time, which cannot be the case given the evolution of a person's identity over time.

(ii) A second approach considers that there is an identity in context, i.e. as many identities as there are identification needs within a society, such as a birth recorded in a civil register, access to an online account via a digital identifier, or a job with the necessary proof of a professional qualification through a diploma.

These two approaches and attempts to delimit identity can be understood in terms of the notions of root identity and extended identity. The former is more important and foundational, but its affirmation is tending to gradually fade away in an ultra-digitized society that seems to be

[43] A phrase freely inspired by Voltaire's maxim: "Every science, every study, has its unintelligible jargon, which seems to be invented only to defend its approaches", in *Œuvres complètes,* Garnier tome8.djvu/323 - Wikisource, available online

slowly valorizing people's extended identity attributes. Indeed, in the age of interconnectivity, more importance seems to be attached to the elements of an extended, secondary identity than to the primary, root identity attributes fixed in a state of law. Since the emergence of globalization, the inflation of human exchanges and interactions has also given rise to a globalization of identities. The digital society is generating upheavals of both form and substance, and information technology is constantly expanding the receptacle(s) of information available to each person in the digital space. As the Franco-Lebanese writer and academician Amin Maalouf points out, "*although the population of the planet has almost quadrupled in a hundred years, it seems to me that, on the whole, each person is more aware than in the past of his or her individuality, more conscious of his or her rights,* (...) more attentive to his or her place in the digital world.)*, more aware of his or her place in society* (...) *of the powers at his or her disposal, of his or her identity* (...)"; "(...) *we can legitimately wonder whether globalization will not reinforce the predominance of one civilization or the hegemony of one power* [such as GAFAM / BHATX[44] or, more broadly, the United States]"[45] . It is therefore vital that a body of legislation[46] frames and protects individuals from any abuse of their online identity. A right to a digital identity is emerging. This phenomenon of digital globalization seems to be beneficial for humanity, as long as it does not lock individuals into identities that they have not deliberately chosen and accepted. In the digital age, the ability to define, collect, present and then verify subsets of identity information in a standardized way that is recognized by online services represents a social and IT process whose aim is to enable each individual to prove online who he or she is among other individuals. Before examining this new space, it is important to define the process that every digital identity undergoes, and which takes place in two distinct stages, the first being identification and the second authentication. The first stage consists in convincing a person that his or her information can be reliably captured by a set of personal digital identifiers referred to as "attributes" or "credentials".
"data". This "attribute" capture is often based on attestations embodied in one or more official certificates - usually physical, such as an identity card or passport - issued and then certified by a public entity that every individual can legitimately trust. So, in principle, at the origin of all identity and identification is a source of public authority recognized by third-party verifiers. In the second stage of authentication, an Internet user shares and verifies - in response to a verification request and in order to access digital services - his or her identification attributes already recorded at the time of registration. In this way, and in theory, by verifying a person's civil status documents and then generating

[44] GAFAM is the acronym for the five largest American Web companies - *Google, Apple, Facebook, Amazon* and *Microsoft* - *which* dominate the global digital market by offering digital identification systems to their users. *BHATX stands* for *Baidu, Huawei, Alibaba, Tencent, Xiaomi, the* five largest Chinese technology companies.
[45] MAALOUF Amin, "Les identités meurtrières", *op. cit.* p.133.
[46] Reference is made to various fundamental rights studied in the course of this research, including the right to privacy, consent to the right to be forgotten or dereferenced specified in the RGPD, secrecy of correspondence or business, the right to identity, the fight against online harassment, defamation and digital rumors.

of personal digital identifiers specific to each Internet user, these digital proofs enable renewed access to said online services, assuring them that people are indeed who they claim to be. While some of these early definitions and considerations of the concept of identity are regularly debated and contested in the social sciences, a certain consensus is emerging on the need to define the notion of identity. As the doctor of philosophy and social sciences Alex Mucchielli aptly proposes, identity would be a "*set of meanings affixed by actors to a more or less blurred physical and subjective reality of their lived worlds, a set constructed by another actor. It is therefore a perceived meaning given by each actor about himself or other actors*"[47] . This definition is general enough to bring out an initial systemic observation specific to identity, enabling us to distinguish ourselves from others by asserting our own singularity. In this way, identity seems contextual, i.e. unique and specific to each situation. For several years now, some legal experts have been talking about "*free informational self-determination of individuals*"[48] , also mentioned in an annual study by the Conseil d'Etat in 2014[49] . In practice, this implies that an individual's social interactions are not conditioned and altered by careless use of their personal data, particularly by trusted third parties. This new form of subjective identity is now, more than ever, the focus of attention and could, in the long term, help redefine the historic role of the rule of law and its institutions in assigning identity. A person is a sum of different motivations, each of which undergoes constant change as a result of social interaction. In practice, social identity is often experienced "(...) *as a whole*"[50] by individuals, i.e., in the event of infringement by a third party, it is "*the whole person who vibrates* [who is infringed]". We thus support a dual vision of identity, both root and in-context, in the light of blockchain technologies[51] and decentralized digital identity (IND), which is explored further below.

1.1.1 The philosophical contours of identity

It seems essential to determine the conditions under which the notion of identity can exist. The American philosopher Quine Willard explains that identity implies an insertion of existence into a thing, a concept or a person: "*there is no entity without an identity*"[52] . This expression means that identity is the very essence of all things, and no definition of identity is possible.

---

[47] MUCCHIELLI Alex, "L'identité", Ed. Que sais-je? PUF 2009, available at the following address
[48] EYNARD Jessica, "L'identité numérique; quelle définition pour quelle protection" , p.39.
[49] EC, Recommendation, "Reinforcing the individual's place in the right to data protection ("informational self-determination") to enable him to decide on the communication and use of his personal data" *Conseil d'Etat, Annual study 2014 - Digital and fundamental rights,* accessed online on November 20, 2021.
[50] MAALOUF Amin, "Les identités meurtrières", *op. cit*. p.34.
[51] The term is used in the plural throughout this study to emphasize the multiple aspects and IT variants of this technology. *See infra*, I, Title 1, 2.3.1.1.
[52] WILLARD Quine, "Relativity of ontology and other essays", 1969, No entity without identity, translated from English by Jean Largeault, Paris, Aubier, 1977, p.35.

nor existence is possible without the prior allocation of an identity. For some individuals, characteristics are easily identifiable, such as their physical traits, while for others they are more complex to detect, such as their psychological traits or their capacity to learn. This is also true of animals, whose capacities may go beyond the mere existence of their bodily identity. Although each living being in a given animal community is genetically unique, the population as a whole possesses a collective faculty of its own: each beaver is unique, but all possess the innate ability to build dams from birth. Here, personal and collective identities exist side by side. This universal aspect of identity was already mentioned by Aristotle:

"(...) *to what is in man technique, wisdom, intelligence corresponds in certain animals some other natural faculty of the same kind*"[53] . Is the notion of identity merely a question of perspective: does a snake that moults retain the same identity during the process of physical transformation? This question can be transposed to human nature, on the sole condition that the snake is also endowed with a "*conscience of its own*"[54] , which is not the case. For humans, consciousness is referred to by medicine as a process of metacognition: "*consciousness is what enables us to know our identity* (...) *which is inscribed in a relational context that makes other brains facing us recognize us as a certain person and not another*"[55] . In line with this principle, French philosopher Paul Ricœur asserts that personal identity is intersubjective, meaning that it always develops in a mutual relationship with other individuals[56] . More precisely, it's a question of not confusing ourselves with others, but of co-constructing ourselves through them. In this way, we are all human beings like others, thanks to others, and at the same time possessing our own "*self*" in the face of "*others*". This relationship of social and empathetic equilibrium gives rise to the notion of social identity, as we see it in our study. According to French sociologist Claude Dubar, there are two main currents of thought concerning the concept of identity, one called "*essentialist*" and the other "*nominalist*"[57] . The first is based on original, almost transcendent beliefs intrinsic to every individual, according to which identity enables a fundamental distinction between individuals, with a form of permanence over time. The second refutes this permanence and specific distinction between individuals, focusing instead on the ways in which identity is identified, i.e. its material elements of expression. A mixed mobilization of these two currents is used in this research to understand people's lived identity as close to reality as possible. Most of the history of Western philosophy considers humans to be persons by virtue of their ability to decide autonomously and consciously, i.e., with the capacity to rationalize their actions according to their own system of values, which is itself defined simultaneously in a way that is consistent with the values of the individual.

[53] BOUFFARTIGUE Jean, "Les animaux techniciens, réflexions sur l'animal faber vu par les anciens", 2006, online, Université Nice-Sophia Antipolis, accessed August 20, 2021.
[54] MUCCHIELLI Alex, "L'identité", *op. cit*. pp.79-80.
[55] GAYON Jean et al, "L'Identité, dictionnaire encyclopédique", Ed. Gallimard, 2020, in *Follio Essai*.
[56] RICOEUR Paul, "Soi-même comme un autre", Ed. Seuil 1990, ISBN 2-02-011458-5, available online
[57] DUBAR Claude, "La crise des identités : l'interprétation d'une mutation", 2010, PUF, pp.2-6, available online

and individual identity. This system of values, which forms the basis of personal identity, is based in principle on the continuity between a person's past and present memory, i.e. on his or her ability to reason, and on his or her own memories and personal experiences[58] . Consequently, the identity that Man can claim exists thanks to his ability to (re)remember the past as much as to anticipate the future[59] . This is also what French neurophysiologist Alain Berthoz referred to as "*mental time travel*"[60] .

However, it's important not to confuse a person's lived identity, i.e. their psychological identity, with their primary and legal identity, discussed below. The former is a representation of identity, partly shapeable, profound and constantly changing. The second does not belong to us, and can represent a form of confinement of our psychological identity[61] . Our unique, global identity is subject to constant confrontation and negotiation between these two identities. Our hypothesis is that identity is constantly being negotiated. In early childhood, as soon as a child begins to learn to speak, the system of identifying and learning one's own name is set in motion. This much broader educational programming consists in grafting qualities and defects onto what we later accept as our identity. According to the Danish philosopher Søren Kierkegaard, this first mechanism of identity creation, of a first identity, contributes to annihilating a person's deepest being: by attributing labels to people, it contributes to annihilating all the other things they could be without these social labels. Given this observation, what are we to make of all these attempts to assign our identities, to which we are constantly subjected? It seems that our identity claims reflect our desire to change certain existing identity claims. Etymologically, identity characterizes two or more beings of the same nature. In Latin, to be "oneself" is designated by the term

The French word for "*ipse*" or "*ipséité" is*[62] . Ipséité thus represents a way of existing and being. It is a form of fidelity to oneself, of autonomous constancy, beyond mere permanence to oneself. For French philosopher Paul Ricoeur, ipséité is a major component of a person's identity. He defines identity in terms of two notions, one "*identity-idem*" and the other "*identity-ipse*". The first represents an identity that is stable over time, unchanged and unchangeable, while the second constitutes a "personal identity".

---

[58] LOCKE John, English physician and philosopher described in 1969 that a "person is an intelligent thinking being, who has reason and reflection, and who can regard himself as himself, the same thing hanging, at different times and in different places", The Works, vol. 1 An Essay concerning Human Understanding Part 1 | Online Library of Liberty, accessed online August 20, 2021.

[59] For John LOCKE, the individual is constituted by the continuity of the body and the person by the continuity of his consciousness: "A person's identity extends as far as consciousness can retrospectively reach any past action or thought" in *Essai sur l'entendement humain*, chap.27, II.

[60] BERTHOZ Alain, "Anticipation and prediction", Odile Jacob, 2015.

[61] In France, a person's pivotal identity (surname, first name, gender) does not belong to him or her. This can lead to identity confinement for some people whose pivotal and primary identity no longer corresponds to their psychological identity (transgender people, people whose surname is difficult to bear). While this example may seem anecdotal when applied to France, it takes on its full meaning in the context of an authoritarian country and state: people's pivotal and root identities can be fabricated in such a way as to enclose them in strictly controlled identity bubbles, subject to a specific vision of identity (illustrated, for example, by the indoctrination of people during the Russia-Ukraine war).

[62] RICOEUR Paul, *op. cit*. consulted on August 18, 2021, available online

a form of maintenance in one's projection of self, despite certain changes in the character of identity over time. To better understand the contours of the philosophical dimension of identity, the philosophical thought-experiment of Theseus' Boat[63] regularly evoked in literature proves invaluable. Used since antiquity, this aphorism has been taken up by many modern philosophers and is named after the Greek hero Theseus. The legend states that his boat was repaired so many times that not a single original part was left. The question is whether rebuilding Theseus' boat plank by plank degrades its original identity. In other words, is it still the same boat as before its restoration? Ultimately, this problem can also be applied to the concept of identity and the definition each individual can give it. These two aphorisms underline a kind of paradoxical link between change and permanence, i.e. between the identity of a thing in the face of its own change over time, to the point of redefining itself in the long term. As a result, the philosophical appreciation of identity seems particularly dependent on a subjective approach, i.e., one that is always based on the perception of the person studying it. The aforementioned French philosopher Paul Ricoeur perceives identity as a "*tracker of individuality"* incubated in a "personal space".

A "*narrative identity"* constructed and asserted in a lasting way, consciously or latently, by each individual[64] . However, the concept of narrative identity is only relevant if we consider that the individual possesses complete freedom of decision, which is not necessarily the case given the many social pressures and constraints that exist during the process of constructing a person's identity. So, does narrative identity characterize a personal illusion that is sometimes self-fulfilling? Are we living in the illusion of our own identity? Are we really the main actor in our own fictional identity in the digital age?

It would seem that this capacity for individual construction of our subjective identity is in fact severely limited and conditioned by the social and educational environment in which each individual evolves. Identity can be circumscribed at several levels of generality, as in the example of two similar objects (glasses from the same factory) with the same apparent generic identity, yet different properties (different models or serial numbers). Philosophy prefers a subjective approach to identity, while law favors an objective one. As French philosopher Vincent Descombes puts it: "To *recognize the 'right of subjectivity' is to see the will to be oneself as a moral attitude. The man who asserts this right - the modern man who adheres to the values of individualism - wants to be responsible for himself. He can only be satisfied with himself if he can attribute to himself, by his own choice, the responsibility for his own life.*

[63] Plutarch, "Lives of Illustrious Men", in *Parallèles, ou vies comparées*, translation by Alexis Pierron, 39p. Available online
[64] TETAZ Jean-Marc, "L'identité narrative comme théorie de la subjectivité pratique. Un essai de reconstruction de la conception de Paul Ricœur", in *Études théologiques et religieuses*, 2014, pp. 463-494. Available at

responsibility for what it is"[65] . Ernest Renan[66] , one of the greatest thinkers and prose writers of the 19ème century, in his famous lecture delivered at the Sorbonne in 1882, provided a response to German nationalism, after the annexation of Alsace-Lorraine, that was historically and philosophically based on an identity-nation "*a great solidarity, constituted by the feeling of the sacrifices that have been made and those that one is still willing to make*", thus combating the model of an ethnic identity. As the German-American historian Ernst Kantorowicz reminded us, the jurists of Edward VI's British crown differentiated between "*the two bodies of the king: a natural body and a political body*"[67] . This aptly demonstrates a conceptual distinction between body and mind. We will argue that this idea of identity segmentation enables us to understand the different components of a digital identity in relation to its various contexts of use. It is possible to distinguish between the identity claimed by the individual and that perceived by those around him or her. According to the German-American psychoanalyst Erik Homburger Erikson, the concept of identity crisis has two inseparable components that make up a person's identity: the objective identity that people recognize in an individual, and the individual's identity in relation to himself or herself, a subjective identity. As a result, the individual will not be accepted by the community to which he or she belongs, if he or she is unable to reconcile these two facets. In modern society, the crisis of adolescence is in fact a crisis of identity, and more precisely of the evolution of a child's identity towards that of an adult. It's worth noting the cultural and social differences that exist between traditional and modern societies, the former subjecting young individuals to ceremonial practices and rituals to symbolize an evolution from child to young adult (the identity crisis is thus ritualized), and the latter attempting to individualize the identity crisis process that a young individual will have to face alone (without rituals) as his or her physical, psychological and social identity evolves. On the one hand, the identity crisis is accompanied and systematized by the social collective, while on the other, it is an individual affair restricted to the family circle. For her part, French philosopher and lecturer Julia de Funès, in her recent book on identity[68] , launches into a critique of all facets of identity, concluding that it is an uncertain concept and that seeking an identity can only lead to a dead end. She proposes individualization, the search for one's own uniqueness, in order to rediscover an individual sense of self. At this point, certain ecosystems in the digital world, such as social networks, represent a new refuge for younger generations who are experiencing inevitable and necessary identity crises. While this digital refuge seems to be quite beneficial in enabling these Internet users to form a society within specific communities, it seems that the management of these communities is subject to excessive computer dependency, and liable to become a source of conflict.

[65] DESCOMBES Vincent, 2013, "Les embarras de l'identité", Ed. Gallimard, location 1801 sur 4825.
[66] RENAN Ernest, "Qu'est-ce qu'une nation?" new reprint in 2023, Ed. 1001 nuits, 50p.
[67] KANTOROWICZ Ernst, "Les deux corps du Roi", 1989, Ed. Gallimard, online, in *Rev. Sci. Soc. Polit. 2, Persée*, consulted August 20, 2021, p.84.
[68] De FUNES Julia, "Le siècle des égarés, de l'errance identitaire au sentiment de soi", Ed. L'Observatoire, 2022.

to be manipulated by online service providers. By influencing these communities through their algorithms, social networks intervene directly in the profound identity construction of younger generations, sometimes without protection against their negative effects, such as harassment, online rumors or personal data breaches. As French philosopher Franck Fischbach explains[69] , the term "alienation" or "*alienatio*" first took on a legal meaning, characterizing, for an individual, a legal act of transfer or dispossession of the ownership of one of his or her rights. In the 19th century, German philosopher Georg Wilhelm Friedrich Hegel evolved this original meaning to designate "(...) *the power to separate oneself from oneself, to make oneself other than oneself, and to take oneself back, to reassert oneself in one's own identity*". In concrete terms, Hegel maintains that a person's personal consciousness can only reach the collective and social consciousness of the world on the sole condition that he or she divests and alienates his or her own consciousness, alienation being "*an evil for a good"*[70] , i.e., a passage that each individual takes in a temporarily negative way, so that his or her identity emerges enriched and adapted to the outside world. Today, the notion of alienation has a strong negative connotation, having been reappropriated in the mid-19th century by successive thinkers[71] . This notion of alienation takes on its full meaning in view of the rapid expansion of our extended identity attributes within a digital universe. And yet, we hypothesize that new IT solutions could limit this phenomenon by giving each person back individual sovereignty and control over their data. Ultimately, the theory of "*sortal identity*" proposed by the Austrian-British philosopher Ludwig Wittgenstein[72] , becomes a preferred avenue for this study. It considers that each criterion of identity depends on its object, while retaining an element of uniqueness. One person's identity differs from another's insofar as both are persons (the person here being the object). Thinking about identity is not simply a matter of thinking in a systematically deterministic way, i.e. fixing identity affiliations for each person, at the risk of locking them into these affiliations. It also means accepting identity as the expression and sharing of different personal and social narratives. Coupled with the concept of "*privacy in context*"[73] described by information science professor Helen Nissenbaum, according to which each information flow must correspond to a context of use in line with users' needs, a vision of identity in context seems to make sense. By extension, this form of contextual identity calls for a compartmentalization of the different parts of a person's identity, which is favored in this thesis in order to form a coherent field of research.

[69] FISCHBACH Franck, "L'aliénation: un concept encore utile aujourd'hui?" Université de Lorraine seminar, Oct. 4, 2021.
[70] GAYON Jean et al, "L'Identité : dictionnaire encyclopédique", 2020, in *Folio Essai*, Gallimard. ISBN : 978207283413.
[71] Reference is made to the earlier work of Karl Marx and Bruno Bauer, evoked by Alex Mucchielli in *L'identité*, p.179.
[72] MUCCHIELLI Alex, *op. cit*. p.673.
[73] NISSENBAUM Helen, *Stanford University Press, 2009*, quoted by Claire Levallois-Barth in "L'identité numérique: quelles définitions pour quelles protections", (under the dir. of) Jessica Eynard, Ed. Larcier, 2020, Dalloz Librairie, p.189.

1.1.2 The sociological contours of identity

Authors such as the aforementioned French philosopher Vincent Descombes help us to understand the inseparable relationship between identity and society*: "Can we dissociate the constitution of the city inscribed in texts* [the legal and political identity of a nation] *from that which is inscribed in hearts* [the social and cultural identity of citizens]*?"*[74] . Acknowledging that identities are the product of precise yet unpredictable social and historical processes helps us to understand the paradoxical scope of this notion on an individual and collective scale. The writer, playwright, philosopher and statesman Johann Wolfgang von Goethe wrote: "It *is in vain that we attempt to express the nature of a thing. We strive in vain to paint the character of a human being; put together, however, his ways of acting, his deeds, and we shall see an image of the character* [of his identity]"[75] . From a historical and social point of view, a person's identity is materialized by his or her first and last names, which represent two stable variables through which a singular and minimal identity can be expressed[76] . The American sociologist Erving Goffman referred to first and last names as *identity carriers*[77] . While all societies and cultures make unanimous use of this same historical method of asserting identity, it should be noted that this designation process varies from one culture to another. Indeed, while it is easy to remember each person's first and last names in small societies, this is more complex in contemporary societies, with reference to the law now permitting double surnames[78] .

For several centuries now, this naming process has been legally supported by a stable civil status. This now written process is institutionalized by virtue of the principles of social stability and legal protection. This can also be explained by the significant demographic growth of populations since the 19th century. This growth has created a strong need for identification on the part of states, whose reliable administrative identification of identities is a key element in the common good of society. For example, it helps to ensure justice for all citizens. In this sense, the permanence of a reliable identification system such as paper enabled administrative authorities to identify, register and track their constituents with relative precision. In France, the family name was gradually introduced in the 19th century. A century later, the forename was added, and its use went beyond simple family transmission - as with the surname - to spread into everyday life in the school, professional and personal spheres. As the American sociologist Anselm Leonard Strauss explains, the first and last names characterize us today in our social and administrative relations, forming "*an indissoluble link between the surname and the given name".*

[74] DESCOMBES Vincent, *op. cit*. location 3858 of 4825.
[75] VON GOETHE Johann Wolfgang, "Traité des couleurs", Ed. Triades, 1973, p.71.
[76] ALFORD Richard, "Naming and Identity" in HRAF.
[77] GOFFMAN Erving**, "**Stigmate: les usages sociaux des handicaps**"**, 1975 consulted online August 21, 2021, p.75.
[78] Law n°2002-304 of March 4, 2002 on the granting of a double surname at birth.

and self-image"[79] . However, this nominative process is not a perfectly reliable identification system, due to the possible and regular existence of homonyms. We therefore assume in this research that no identification system will ever be perfect, although current identification mechanisms are particularly effective.

Sociology recognizes that relational mechanisms are at the heart of the identity-building system within communities, groups and societies in general. These relational logics are based on a triple characterization[80] , the groups outside us ("*they"*), the internal groups to which we belong ("*we"*) and, finally, the relationship maintained between these first two groups (the relationship between "*they*" and "*we"*). This representation enables us to consider how people identify themselves collectively through their collective differentiation. This is how national, professional and personal identities are created. Depending on the society studied, there are countless groups to which people belong, whose claimed identities are often complex to grasp, as they are experienced and felt both subjectively and collectively. Historically, identity in the sense of identity is a notion developed in 1970 by the American historian Philip Gleason[81] . At the time, he noted the massive use of the term identity by many social scientists, yet they were unable to define it precisely: "*Identity is one thing, it's what it is*". Gleason shows that the concept of identity first appeared in the American social sciences in 1955 to enable individuals (Americans) to situate themselves within a society of other social groups to which they belong, thus forming a national identity, notably through their distinctive characteristics, religious identity, ethnic origins. This idea is similar t o Paul Ricoeur's concept of narrative identity, mentioned earlier, i.e. an identity constructed by the individual who decides to choose how to (re)interpret his or her past. It appears as

"*a pathological phenomenon, a source of 'confusion' and disorientation"*[82] with which each person must consciously internalize who they are, and manage this conscious and unconscious representation in their social interactions, now digital. Finally, as Philip Gleason has shown, the term identity is a source of embarrassment, as it is used in the American social sciences without even possessing a precise definition. As a result, its use and meaning have taken on a number of sometimes opposing definitions, which are now to be found in our common language. If identity seems to be a fundamentally personal and intimate element, the social sciences seem to qualify this first impression to emphasize the social and external dependence of a personal identity on the world. The famous maxim "*Man is an animal by nature political"*[83] from

[79] STRAUSS Anselm, "Miroirs et masques, une introduction à l'interactionnisme", 1993, Revue des sciences sociales du politique, accessed online August 21, 2021, pp.142-146.
[80] MUCCHIELLI Alex, *op. cit.*
[81] GLEASON Philip, "Identifying Identity: a semantic history", in Journal of American History, vol. 69, no. 4, March 1983, pp. 910-931.
[82] DESCOMBES Vincent, *op. cit*. Location 463 of 4825.
[83] JAULIN Annick, "La nature de l'animal politique humain selon Aristote", Éd. Sorbonne, 2017, available online.

the Greek philosopher Aristotle, would thus state a natural law according to which Man is destined to live in society. Six centuries later, the German sociologist Norbert Elias would add that "*we can only oppose the individual and society as two entities at the level of language*"[84] . This observation is also shared by the sociologist Émile Durkheim, for whom "*man is only a man because he lives in society*"[85] . Culture is thus at the heart of the creation and maintenance of all social life, and by extension of all collective or individual identity. Ultimately, to find one's identity and belonging is to form a community. The famous French anthropologist Claude Lévi-Strauss testifies in his book "La pensée sauvage" (1964) to the way in which the individual singularity of people does not contradict their integration into social groups. From his anthropological point of view, he explains how this process of integrating individuals from outside a society (foreigners or a new generation) disrupts the established order. The community must systematically provide or make room for the individuality of each new member of its group. This observation is supported by French author and academician Amin Maalouf, who believes that it is essential to introduce and promote a concept akin to that of solidarity identity, i.e. to encourage people to put themselves in the place of their fellow human beings by cultivating multiple reciprocal affiliations.

A person's social identity thus encompasses all the memberships that together make up his or her personality, but whose combinations and priorities are constantly changing: "*while each of these elements* [of belonging] *may be found in a large number of individuals, the same combination* [of belonging] *is never found in two different people, and this is precisely what makes each person rich, his or her own value, what makes each being singular and potentially irreplaceable*"[86] . According to the Indian philosopher Amartya Sen, every individual has several identities
"Since each person possesses several identities, each time he or she must choose, from among the different groups that can claim allegiance, the one that will prevail on a given occasion"[87] . As a result, identity is above all a social phenomenon, enabling people to claim social identities according to two allegiances: one class-based, corresponding to a common criterion shared by individuals, and the other communal and social. Combined, these two affiliations form social identity. Separated, they do not systematically create a sense of identity sufficient for individuals to form a social group, a source of identity claims that are understandable and accepted by all. In the sections on self-sovereign digital identity and Metavers below, we see that these two types of belonging are probably lacking in their mass adoption, unlike the Bitcoin blockchain, which represents a new form of quasi-nation.

[84] DUMA Jean, "Histoires de nobles et de bourgeois: Individus, groupes, réseaux en France. XVè-XVIè siècles", Presses universitaires de Paris Nanterre, p.187.
[85] DURKHEIM Emile, "Education and Sociology", PUF, Coll. Quadrige, new edition 2022, p.55, online at
[86] MAALOUF Amin, *op. cit*. p.17.
[87] DESCOMBES Vincent, 2013, "Les embarras de l'identité", Ed. Gallimard, location 179 sur 4825.

technocratic[88] . Karl Marx said that "*it is not the consciousness of men that determines their being Conversely, it is their social being that determines their consciousness*"[89] . According to leading social scientists such as Austrian political scientist Joseph Schumpeter and French sociologist Pierre Bourdieu, there are three typologies of class identity[90] : temporal (the ability of a social class not to merge with others over time), cultural (all forms of cultural, political, social, economic or even physical claims specific to a social class) and collective, reflecting the higher interests of the collective and its capacity for representation and action. As mentioned above, collective identity took precedence over the individuality of each person, with all action viewed through the common prism of "*we"*. In contrast, contemporary societies tend to set up a personal, individualistic and autonomous identity as a goal and figure of social success. French sociologist Emile Durkheim referred to this social and cultural phenomenon as a cult of the individual, whereby society cedes some of its collective values in favor of personal ones. We'll see that many IT applications linked to 3.0 technologies knowingly or unknowingly exacerbate a new form of individual, community and financial worship, with Metavers and NFTs, for example, being studied later.

However, traditional and contemporary societies remain structured social organizations. Canadian philosopher Charles Taylor believes that, from the 18th century onwards, our modern, Western societies entered a process of "*desocialization*", whereby "*social life*" and the "social order" were replaced by "social organization".

As a result, "*social affairs*" have become progressively rationalized, giving way to individual pressure and social influence[91] . Thus, in our modern societies, individuals are comfortable with free self-determination and the unconscious de-socialization of their identity, in contrast to traditional societies. Complementing this, French anthropologist Louis Dumont explained that the modern individual "*thinks* himself *into an individual*", i.e. he possesses the power to decide on the conditions for self-satisfaction and self-esteem. In a way, this is the individual's right to identity emancipation, i.e. the ability to define himself according to his own conventions and wishes. If this possibility has never been so true in the digital age, particularly in Web 3.0, the daily influence of certain digital networks on our identity has never been so important and paradoxical. Over the past few years, a new sense of identity has emerged, with a desire to de-gender people's identities, i.e. to remove the categories of masculine and feminine from certain physical and digital contexts. So, two subsidiary questions seem important on the subject: why do gender identities exist? Are they still relevant today? In France and Europe, gender identity is the fruit of our history and culture.

---

[88] V. Appendix 3, Focus 1 to 6.
[89] EGE, Ragip, "À propos de l'ouvrage de Karl Marx: Contribution à la critique de l'économie politique. Introduction aux Grundrisse dite 'de 1857'", 2016, in *Cahiers d'économie Politique*, available at.
[90] GAYON Jean et al, *L'Identité : dictionnaire encyclopédique*, 2020, Folio Essai, Gallimard. ISBN : 9782072834134.
[91] DESCOMBES Vincent, *op. cit.* location 2088 of 4825.

social and religious. Used since the 12th century[92] , these terms are still widely used today, including on official identity documents. The aim is to abolish the use of gender in civil and legal identity documents - in line with the recent abolition of the use of the term "Mademoiselle"[93] by public institutions - because this gender distinction is no longer necessary or justified, but simply the fruit of our history and culture. Doing away with genders would provide a simple response to a twofold social and IT problem: the growing number of citizens who want to be able to change gender at any point in their lives, because they don't recognize themselves in either of the two traditional categories ("man" or "woman"). Its deletion would make it possible to introduce a conceptual principle of minimizing the identity of individuals, by helping to reduce the large quantity of personal attributes and data that can be collected (for example, only essential attributes such as biometrics could be collected). In this way, a person's function would no longer take precedence over the person, who would then be more freely claimed. In conclusion, it seems that the concept of identity is above all an effective, if complex, means of evoking the diversity of human beings and their singularities. If an individual wishes to be perceived at his true worth, it's a question of enabling him to express what he believes to be the most valuable aspect of his uniqueness. We are studying how decentralized digital identity could revive the utopia of an individually and collectively sovereign and *agentive* identity[94] . However, giving Internet users too much autonomy and responsibility could also lead to uncontrolled excesses. We will attempt to strike a balance between the importance of this theory and the appropriate, innovative IT tools currently available.

1.1.3 The legal contours of identity

Identity is defined on an international scale in a complementary way by several transnational organizations. In 2015, a group of experts attached to the United Nations and working on the establishment of sustainable development goals on an international scale published a list of indicators, one of which stresses that "*providing legal identity for all (including birth registration) by 2030 is a goal shared by the international community in the framework of the*

[92] DEVELEY Alice, August 21, 2018, "'M.', 'Mr' : ces abréviations de titres de civilité à ne plus écorcher ", in *Le Figaro*, at the following address.
[93] Circular no. 5575/SG of February 21, 2012 on the removal of the terms 'Mademoiselle', 'nom de jeune fille', 'nom patronymique', 'nom d'épouse' and 'nom d'époux' from administrative forms and correspondence, available at.
[94] GAYON Jean et al, "L'Identité : dictionnaire encyclopédique", *op. cit*. p.169. Agentivity is the capacity of an actor to act in a given environment. In sociology, an agent is an individual who engages with the social structure. The feeling of agentivity characterizes a sense of control over one's own actions and, by extension, over events in one's social environment.

Sustainable Development Goals (target 16.9)"[95] . In 2018, the International Telecommunication Union (ITU) referred to identity as "*the representation of an entity in the form of one or more attributes that sufficiently distinguish the entity or entities in a context*"[96] . In 2019, the International Organization for Standardization (ISO) defined it as "*a set of attributes related to an entity*"[97] completing "*identification is a process of recognizing an entity in a particular domain as distinct from other entities*"[98] . Paradoxically, the Declaration of the Rights of Man and of the Citizen (DDHC) neither mentions nor defines identity. Nevertheless, it indirectly recognizes a right to identification in Article 6
"(...) *all citizens, being equal in his eyes, are equally eligible for all public dignities, positions and jobs, according to their ability, and without any distinction other than that of their virtues and talents*"[99] . The right to have an identity and to be identifiable therefore seems to be indirectly recognized, without any precise definition of the notion of identity. These initial definitions offer a common legal basis for approaching the notion of identity from a general, abstract angle. Since the identification of individuals is an essential process for granting them access to services of all kinds, we need to define its material elements more precisely. The role of the law is to set the conditions for the creation of physical and digital identity, one of the major components of which is based on dematerialized personal attributes in the form of data circulating online. Access to certain services or social interactions requires prior identification of individuals or users. In principle, these identification systems are provided to citizens by the State, and are governed by law. The aim is to build a large-scale identification system, which requires a high level of trust on the part of citizens, institutions and businesses. Without total transparency and legal confidence, a climate of mistrust may develop or persist towards any technical identification solution, given that identity is a sensitive area that directly involves the personal and psychosocial sphere of each individual.

Universally, most states around the world position themselves as the primary provider of identity for individuals, notably through a paper or plastic physical identity document and a birth certificate[100] . The latter is based on a physical and/or electronic register that is kept

[95] World Bank Group, *identification for development*, accessed online August 25, 2021, "Providing legal identity for all (including birth registration) by 2030 is a target shared by the international community as part of the Sustainable Development Goals (target 16.9)".
[96] International Telecommunication Union (ITU), "Telecommunication Standardization Sector, X.1252, Baseline identity management terms and definitions", April 2010, "identity is the representation of an entity detailed enough to make the individual distinguishable within a context", p.4, 2018, in *Digital Identity Roadmap Guide.*
[97] "Identity is a set of attributes related to an entity", ISO/IEC 24760-1.3.2.1
[98] "identification is the process of recognizing an entity in a particular domain as distinct from other entities".
[99] Déclaration des Droits de l'Homme et du Citoyen (DDHC) de 1789 | Conseil constitutionnel, consulted online on August 25, 2021.
[100] BENSOUSSAN Alain, "Today, information [about a birth] is communicated electronically to the public administration by the maternity doctor as soon as the baby is born. A national identity number is assigned", in *L'identité numérique 5.0*, Bensoussan Avocats, Ed. Lexing, p.16.

updated by the State and its administration over time. The person legally responsible for the child can receive an attestation or certificate which therefore represents the information in this official register, for which the State is the guarantor. This information, stored as part of the birth registration process, mainly comprises name, date and place of birth, nationality, parent(s) and sometimes other complementary characteristics (eye color, sex, height). However, while legal doctrine defines identity as "*all the elements which, under the terms of the law, contribute to the identification of a physical person (surname, first name, date of birth, parentage)*"[101] , some legal experts note that there is already a hierarchy of importance between certain material elements of identity. Indeed, the surname, first name and date of birth seem to take precedence over all others.

This is the "*pivotal point*"[102] in relation to other criteria, such as place of birth. Because personal civil status materializes and confers an identity and legal existence on people[103] , this "*minimum identity core"*[104] grants them a legal personality and status by giving them access to voting rights and subjecting them to obligations (tax assessment, etc.). As a result, a person's civil status gives rise to an identity that we refer to throughout this thesis as primary, root and legal. For legal entities under French law, the legal identity of an organization arises when the clerk's office of a commercial court registers certain minimum information (Kbis, legal representatives, legal form, articles of association, registered office) enabling an organization to be identified in the Trade and Companies Register (RCS) at the 227 French commercial courts. The identity of individuals and companies is thus based on human, administrative and IT processing. While the scope of this research is primarily concerned with the identity of natural persons, the identity of legal entities is also examined through the prism of decentralized digital identity, as well as in a section dedicated to digital objects.

Titles and official identity documents represent material supports that are actually extended and extracted from the civil register, which remains the sole source of truth for the legal identity of individuals[105] . These documents enable citizens to prove their nationality and related rights. They facilitate handwritten proof of their legal identity. Each document has its own specific purpose: a passport is used to "*pass through ports*", i.e. to travel, a national identity card (CNI) enables free movement within the national territory, and a voter's card enables citizens to express themselves through democratic voting. The history of the development of these identity media is worth recalling, in order to fully understand the current and future challenges of their dematerialization. The history

[101] EYNARD Jessica, "L'identité numérique; quelle définition pour quelle protection?", Coll. Larcier, 2020, Dalloz Librairie.
[102] This term is introduced in Deliberation no. 2015-254 of July 16, 2015, issuing an opinion on a draft order creating a personal data processing operation by the interministerial directorate for information and communication systems for the teleservice called FranceConnect
[103] Date of birth is used to define a person's age and therefore legal capacity. Domicile links a person to a territory and its associated jurisdiction.
[104] BERNARD Alain, "L'identité des personnes physiques en droit privé", consulted online 26/08/21, p.155.
[105] Reference is made to the birth certificate, which represents a cornerstone for the legal recognition of a natural person.

of identity documents has its roots in the boom in migratory movements, which rendered ineffective the traditional methods of identification based on first and last names mentioned above. The latter were deemed unreliable, as they depended on the knowledge and memory of individuals. The first attempt to improve the identification system came in the 16th century, with the Guillemine ordinance decreed in 1539 by François 1er[106] . This introduced and imposed standardization of the French language for all administrative and legal acts of the time, notably by abolishing the use of Latin for these acts. As a result, and under the guise of strengthening monarchical power, it required parishes throughout France to record all marriages, births and deaths in parish registers. Civil status appeared in its first form, and was instituted in its modern form after the French Revolution[107] . The Third Republic marked a turning point in the identification of the State with its citizens. In addition to the systematic use of civil status[108] to issue identity papers to French citizens, the law of August 8, 1893 on the residence of foreigners in France and the protection of labor in France[109] required immigrants to register in order to access and prove their right to residence. This first law, a precursor in terms of compulsory identification, was later supplemented in 1917 by a national identity card imposed on all colonial workers. After 1918, the concept of the national identity card was extended to the entire French population, in order to guarantee reliable identification and official citizenship for the French. From then on, a person's identity and civil status were two inseparable concepts. Yet their links are regularly called into question in order to designate other realities, and to express the need to claim new affiliations materialized by new, extended attributes of personal identity. If the law organizes its own truth with regard to people's *primary, civil* identity, can it be any different for people's *subjective, secondary identity?*

Law professor Alain Bernard distinguishes between *permanent identity* (fixed by law) and *claimed identity* (the role fixed by society), the former being necessary for the latter and the latter inseparable from the former. He thus sees society as "*a gigantic net*"[110] through which each person is linked to the others, in a more or less direct and complex way. The indeterminacy and legal unavailability of identity in French law can be explained by the diversity of functions it plays in the legal life of individuals. This indeterminacy is due to the constant evolution of the notion of identity, which legal professionals prefer to limit to certain material and immutable elements. With a similar ambition, the unavailability of the identity of

[106] This Ordinance is the oldest piece of legislation still in force in France; Ordonnance du Roy sur le fait de justice, consulted online on 21/08/2021.
[107] BENSOUSSAN Alain, lawyer, "It was the French Revolution that took the keeping of registers out of the hands of the Catholic Church and entrusted it to the State, thus creating the so-called regalian identity", in *L'identité numérique 5.0*. Ed. Lexing, p.16.
[108] In the form of central files held by the Republican powers.
[109] Loi du 8 août 1893 relative au séjour des étrangers en France et à la protection du travail national, consulted online on August 21, 2021.
[110] BERNARD Alain, *op. cit.* p.133

This is complementary to its legal indeterminacy: in principle, it makes it complex and unavailable to modify one or more material elements of a person's identity (surname, first name)[111] . For example, the reading of French citizens' biometric data on the chips in their passports and electronic national identity cards, studied below, is legally authorized[112] only by sworn state agents and not by the physical holders of the biometrics, which demonstrates the unavailability of our identities, particularly with regard to their accessibility[113] . However, it seems that "(...) little by little, *the law has given way to a desire, albeit controlled, to interfere in the main elements of status, namely surname, first name and gender*"[114] . Although the association of a surname and a first name may still be affected by homonymy[115] , it should be noted that this association still makes an individual relatively unique and easily identifiable, thanks in particular to biometrics in the cases provided for by law. Digital identities (pseudonyms and social network avatars) sometimes call into question this uniqueness of a person's identity, despite the fact that only their attributes and civil identity data enable them to carry out everyday legal acts. In most situations, it seems that civil status and personal identity are subject to the principles of reciprocal indissociability, immutability and unavailability. However, personal identity - thanks to advances in digital identity - seems to be in the process of emancipating itself from the civil status that gave birth to it: a new form of chosen digital identity is emerging, whose contours are sometimes as decisive as a civil identity, depending on the digital ecosystems in which it manifests itself, in Metavers and social networks in particular. Civil status also faces constraints and limitations, particularly as regards the reliability and authenticity of material information derived from it, such as ID cards and passports, as well as documentary fraud linked to civil status certificates that are not sufficiently secure, lacking biometric security components or holograms. In addition, it is complex to update identity documents, which can lead to confusion between people's civil status and their identity documents, which are in reality no more than derivative media summarizing certain minimum information about their civil status at a given point in time.

---

[111] Under French law, it is possible to change one's surname directly with the Minister of Justice, in a completely paperless process, and only in the case of a legitimate reason (articles 61 to 61-4 of the Civil Code). In Great Britain, this process is administratively simpler (a short form is required), faster (1 to 4 weeks) and less costly (~£42). The process is public and enables the legal use of a new name, a choice made by over 85,000 people every year in Great Britain.

[112] "Only national police officers in charge of border control, who are individually designated and specially authorized, and who are officers or agents of the judicial police, have access to information resulting from the interconnection between PARAFES and the wanted persons file and the Schengen information system [biometric database].", Fiche Question. Available at the following address

[113] SENAT, Proposition de loi relative à la protection de l'identité, 1er June 2022, "[...] limit to authorized agents the possibility of reading fingerprints on identity documents to ensure that they correspond to those of the bearer", available at the following address

[114] SIFFREIN-BLANC Caroline, "L'identité des personnes: une identité pour soi ou pour autrui", accessed online August 26, 2021, 2016, in *Presses de l'Université Toulouse 1 Capitole*, p.3.

[115] Homonymy can, however, be ruled out by other root identity attributes recorded in the civil status (domicile, date and place of birth, etc.).

Without going into too complex a classification of the types of personal data that can exist, it is accepted by legal experts that the aggregation of a few personal data is more than sufficient to characterize and trace the root or extended identity of a person. For example, personal data was characterized in 2007 by the "article 29" working group[116] on data protection: "*It should be noted that while identification by name is, in practice, the most widespread means, a name is not always necessary to identify a person, particularly when other* [digital] *'identifiers' are used to distinguish someone.* (...) *The individual's personality is thus reconstituted in order to attribute certain decisions to him or her. Without even asking the person's name and address, we can characterize him or her according to socio-economic, psychological, philosophical or other criteria, and attribute certain decisions to him or her, insofar as the person's point of contact (the computer) no longer necessarily requires the revelation of his or her identity in the narrow sense of the term. In other words, the possibility of identifying a person* [online] *no longer necessarily implies the ability to know his or her identity*"[117] . With the multiplication of technological devices, coupled with the evolution of increasingly digitized social practices and interactions, individuals have never issued so much data[118] . At Community level, Article 8 of the European Convention on Human Rights (ECHR), which came into force on September 3 1953, laid the foundations for the right to respect for private life and, by extension, for the identity of individuals: "*Everyone has the right to respect for his private and family life, his home and his correspondence*"[119] . Once a person has this right at birth, the foundations of personal identity, home, family and social interaction are respected. Gradually, the ECHR adapted and broadened the definition and protection of identity in the face of successive social, political and technological trials and tribulations. It "*frees* itself *from all limitations in all existential choices - sex, body, life and death - of the individual*"[120] , as "*the notion of private life includes elements relating to a person's identity such as name*". It seems that technological developments and social preconditions are increasingly coming up against European case law in favor of the recognition of a universal human identity. Indeed, European case law lays the foundations for a right to personal autonomy "*although it has not been established in any previous case that Article 8 of the Convention entails a right to self-determination as such, the Court considers that the notion of personal autonomy reflects an important principle underlying the interpretation of the guarantees of Article 8*"[121] . A s Claire Levallois-Barth, senior lecturer and teacher at the University of Paris, explains

[116] On May 25, 2018, the European Data Protection Board (EDPB) replaced the 'Article 29' Working Party, in "L'identité numérique ; quelle définition pour quelle protection ?", Jessica Eynard, Coll. Larcier - Ed. Dalloz Librairie Paris.
[117] *Op. cit,* Opinion 4/2007 on the concept of personal data, consulted online on August 30, 2021.
[118] "Total data volume worldwide 2010-2025" published June 2021 in *Statista* online, accessed August 30, 2021, translated from English "181 zettabytes of data volume created, captured, copied and consumed worldwide from 2010 to 2025"; International Data Corporation estimates that the global data sphere will grow from 33 zettabytes in 2018 to 175 zettabytes in 2025.
[119] It should be noted that, unlike the UDHR, whose scope is more symbolic and moral, this Convention enables any European citizen to invoke it to defend himself or herself.
[120] EYNARD Jessica, "L'identité numérique; quelle définition pour quelle protection?" *op. cit.* p.31.
[121] ECHR, April 29, 2002, Pretty v. United Kingdom, 2346/02, in *Revue générale du droit*, consulted online on August 30, 2021.

researcher at Télécom Paris, "what's at *stake here is respect for each individual's free will, and therefore for our freedom of choice. The very possibility for people to present themselves as they wish, to live their lives by defining these alternative identities, contributes to respect for their fundamental freedoms, notably freedom of expression and communication, membership of a community or political activity*"[122] . Thus, in the sense of Community law, identity seems to be protected and encouraged in its development beyond the national definitions of civil identity usually accepted by member states. To illustrate, the ECHR declares "*the right of everyone to establish the details of his or her identity as a human being*", to the point of noting the ubiquity of this notion in European case law. The ECHR thus acknowledges respect and legal certainty, not only for the notion of identity in the sense of the means contributing to its identification (legal identity), but also for the various components of social identity: "*the Court is thus building a genuine identity policy, based on tolerance and acceptance of differences*". In short, the ECHR appears to be moving towards the conceptual establishment of a universal identity accessible to all, guaranteeing equal treatment and recognition, freedom from discrimination, and autonomy for European citizens.

1.1.3.1 The right to identity: rationale and founding international texts

The right to identity refers directly to the right of every child to be assigned a civil identity from birth. This attribution enables the individual to benefit from a legal personality, which is indispensable for effective and lasting legal protection. Identity is indeed a prerequisite for all other rights, and remains a major challenge for any constitutional state[123] . A person's birth certificate can be seen as a visa for a right to life: it materializes the individual's legal existence and enables him or her to prove it. The birth certificate thus represents the founding act of civil status, and its subsidiary and future acts (marriage, divorce, death). It includes the person's first name, surname, sex, date and time of birth, place of birth, parents' names, dates, occupations and places of birth. Yet every year, some 51 million births go unregistered, representing some 166 million children worldwide. This scourge of unregistered children has disastrous social and economic consequences for society, including difficulties in accessing public services (justice, health, education) and private services (banking, employment), to name but a few. In the majority of cases, these situations result from a lack of registration within a trusted civil registry. It would be more accurate to speak of identity rights in the plural, as the single conception of

[122] EYNARD Jessica et al, "L'identité numérique; quelle définition pour quelle protection?" *op. cit*, p.187.
[123] "Without a birth certificate to prove his or her identity, a child may be deprived of access to his or her most fundamental rights (...) a legal identity at birth, a right for every child", in *IN Groupe's online Observatory*, May 19, 2022, available at the following address

identity, which brings together a series of international conventions that enshrine and protect certain fundamental human rights, including the right to identity. This right to identity is covered by several international treaties and conventions, illustrated below in chronological order:

(i) The Geneva Declaration on the Rights of the Child[124] represents the first founding text to recognize, in five articles, the importance of a right to identity for every child. This international declaration (non-binding) was adopted on September 26, 1924 by the League of Nations (League)[125] . The text lists the fundamental needs of the child, and the responsibilities which in principle fall to adults to meet them. It thus expresses recognition of the child's right to development, assistance, relief and protection.

(ii) Because of its universal vocation, the Universal Declaration of Human Rights (UDHR) represents a second recognition, becoming a cornerstone of international law (not exclusively reserved for children) which recognizes a right to legal identity: "*Everyone has the right to recognition everywhere as a person before the law.*
"[126] . A decade later, this principle was specifically applied to children by virtue of Rule 3 of the Declaration of the Rights of the Child of November 20, 1959: "*the child has the right, from birth, to a name and a nationality*"[127] .

(iii) However, it wasn't until the ratification and adoption of the International Covenant on Civil and Political Rights (ICCPR) on December 16, 1966, that the UDHR and the Declaration of the Rights of the Child conferred certain binding provisions on its signatory parties (almost half a century elapsed between the Geneva Declaration and the ICCPR).

(iv) While these few framework treaties have laid the legal foundations for a form of international identity law, it must be admitted that it is the International Convention on the Protection and Promotion of the Diversity of Cultural Expressions that has the greatest impact.

[124] Geneva Declaration on the Rights of the Child, 1924, in *Humanium*, consulted online on April 30, 2021.
[125] The role of the League of Nations was to ensure the maintenance of peace in the world: to fight for the rights of children during conflicts, for the prevention of wars, and for the negotiation and resolution of conflicts. After the Second World War, the League was replaced by the United Nations (decided at the 1945 Yalta Conference).
[126] *Ibid.* Art. 6, accessed May 3, 2021.
[127] Declaration of the Rights of the Child of November 20, 1959 - Full text, in *Humanium*, consulted online on May 3, 2021.

on the Rights of the Child (CRC)[128] has been the cornerstone of the CRC since 1989. It represents an unprecedented legal consensus within the international community, and is the most ratified human rights convention in history, with 195 ratifying states except the United States and Somalia[129] . The CRC and this right to identity for children were initially initiated by the United Nations Children's Fund (UNICEF). On the one hand, Article 7 of the CRC reaffirms the guarantee of a right to a name and nationality for every child in the signatory states[130] , and on the other hand, Article 8[131] , requires signatory states to ensure that these same rights are respected within their respective jurisdictions. This convention therefore has a significant symbolic impact which, coupled with an unprecedented legal constraint[132] , makes it a tool in the service of a right to identity. From the 2000s onwards, the desire to adopt and apply a universal right to identity was reinforced. On May 10, 2002, the United Nations General Assembly adopted resolution S-27/2, entitled "*A world fit for children"*.

"In this document, governments reaffirmed their common commitment to "establish *systems for registering all children at birth or shortly thereafter, and to respect the right of every child to a name and nationality, in accordance with national legislation and relevant international instruments*"[133] .

Despite these solid legal and international foundations, it has to be said that, to date, one billion people have no official document to prove their identity. If nothing changes between now and 2030, around a third of the world's countries will have to accelerate their policy of birth registration and the provision of legal identity for their citizens in order to meet target no. 16.9 of the Sustainable Development Goals (SDGs). This same United Nations General Assembly goal n°16.9 was announced at UN headquarters in September 2015 in order to establish a "*universal, integrated and transformative* program *that will lead us to a better world*", according to a statement by

[128] Adopted on November 20 1989 and entered into force on September 2 1990, thirty years after the Declaration of the Rights of the Child of November 20 1959.

[129] BENNOUNA Mohamed. La convention des Nations Unies relative aux droits de l'enfant, in *Annuaire français de droit international*, volume 35, 1989. p.433-445. Signed by France on January 26, 1990, ratified on August 7, 1990 and entered into force on September 6, 1990.

[130] Art 7-1 and 7-2 of the CRC: "1° The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality and, as far as possible, the right to know and be cared for by his or her parents; 2° States Parties shall ensure the implementation of these rights in accordance with their national law and their obligations under applicable international instruments, in particular in cases where the child would otherwise be stateless.
v. unicef.fr

[131] Art. 8-1 and 8-2: "1° States Parties undertake to respect the right of the child to preserve his or her identity, including nationality, name and family relations as recognized by law, without unlawful interference; 2° If a child is illegally deprived of some or all of the elements of his or her identity, States Parties shall provide appropriate assistance and protection, with a view to re-establishing his or her identity as soon as possible.

[132] Art. 41: "If a provision relating to the rights of the child contained in the national or international law in force for a State is more favorable than the analogous provision in this Convention, the more favorable standard shall apply". [133] UN, "A World Fit for Children - General Assembly - 6th plenary meeting", downloaded online or accessible here on May 3, 2021.

former UN Secretary-General Ban Ki-moon[134] . In other words, legal identity is, and will remain by 2030, at the heart of the legal concerns of many international institutions. However, according to UNICEF, "*it is clear that unless the pace of birth registration accelerates significantly in all countries, particularly in Africa, we will miss the 16.9 target of the SDGs by a wide margin*"[135] . Similarly, the Human Rights Council (HRC) adopted provision no. 43/L.3 on June 19, 2020, declaring itself "*1° deeply concerned that* (...) *237 million children still do not have a birth certificate despite the efforts that are being made* (...)*; 2° Reminds States of their obligation to register all births without discrimination of any kind, and also reminds them that every child should be registered immediately after birth in the country where he or she was born,* (...) *in accordance with international human rights law* (...); 3° *Reaffirms that guaranteeing everyone a legal identity, in particular through birth registration, by 2030 can help to prevent, among other things, poverty, marginalization, exclusion* (...) "[136].

Organizing birth registration is essential to the social, democratic and economic development of a country. To achieve this, it must be technically capable of identifying and then administering its population, i.e. of forming a nation, notably by personalizing identity documents in the nation's colors. In reality, the State is as much the guarantor as the beneficiary of personal identity. To achieve this, public resources such as taxation must be stable, which means identifying its citizens at source, if possible from birth. Rigorous knowledge of the population makes it possible to build a civil registry that benefits those entitled to it, and a virtuous circle is established thanks to faithful identification. This identification of individuals is also necessary for various macroeconomic, budgetary or monetary decisions, projections and policies. When a state lacks an effective identification system, it can jeopardize its democracy, because in the absence of a reliable civil registry and corresponding official documents, electoral fraud can flourish. In such situations, the legal identity of individuals becomes a deceptive facade, and sometimes an illusion that generates mistrust among citizens.

With no legal existence or protection, and no access to education, children are exposed to all kinds of trafficking: forced labor, organ trafficking and human trafficking, physical and psychological abuse, to name but a few. More generally, the absence of a legal identity has a destructive social and psychological impact throughout a child's life. The fact of not being registered can cause a child to feel excluded, especially if he or she belongs to a community where

[134] "General Assembly adopts ambitious sustainable development plan to 'transform our world' by 15 years", Coverage of press release meetings, in *UN Press*, available at
[135] Workshop "Mission 100: towards 100% legal identity by 2030", ID4AFRICA funded by UNICEF, concept note for the June 16, 2022 workshop.
[136] Birth registration and everyone's right to a legal personality - Human Rights Council, consulted on

other members are registered and enjoy the benefits of registration. In principle, a civil registry requires a condensed territorial distribution and must be able to adapt to demographic changes. This requires a fluid relationship between registration centers such as hospitals, town halls and civil registries. By 2020, the United Nations High Commissioner for Refugees (UNHCR) estimates that there will be 10 million stateless people in the world, a third of them children[137] . As a result, setting up reliable national identification systems remains an IT, economic, social and legal challenge for many countries. This economic challenge is directly linked to the possibility of deploying infrastructures dedicated to personal identification. UNICEF notes "*a correlation between national income per capita and the implementation of an efficient civil registration system in a country. The higher a State's public budget, the more it will be able to set up civil registry centers (including mobile centers for the most inaccessible regions), equip them (particularly with digital equipment), and recruit and train civil registry agents*"[138] .

In many countries, the issuing of identity documents such as birth certificates requires an administrative act that citizens have to pay for, particularly in sub-Saharan Africa "*where the poorest 20% of children are half as likely to be registered at birth as the richest children*". However, the administrative cost in question is only one direct aspect of the expenditure, often accompanied by indirect costs that are all linked to the same process (such as the transport required to register one's civil status, the loss of parents' wages during their travel and absence from work, the loss of identity documents). The economic aspect is closely linked to legal considerations, i.e. the law in force in the above-mentioned countries. It seems that only a transparent legal system can offer national registration virtually free of charge for its citizens, and especially for children. In reality, many countries still have disparate, even obsolete, legal regimes, in terms of both registration costs and administrative delays in issuing identity documents where they exist. The aforementioned economic aspect is therefore a determining factor in the implementation and legal framework granted to any civil status. What's more, this is often accompanied by IT constraints in addition to the aforementioned legal constraints. In principle, to guarantee the protection of citizens' fundamental freedoms, a digital civil registry must comply with technical specifications ensuring the conformity and protection of identity information. In practice, many countries have set up systems that fail to meet these criteria, whether in terms of IT security, technical compliance or legal protection of personal data. The consequences of these shortcomings or inadequacies can be serious: theft of personal data,

[137] "L'apatridie", published on June 5, 2020, in Forum réfugiés, consulted at the following address
[138] Assemblée nationale, Rapport d'information n°3349 déposé par la commission des affaires étrangères, en conclusion des travaux d'une mission d'information sur les enfants sans identité (Mme Laurence Dumont et Mme Aina Kuric), accessed online on April 29, 2021.

discriminatory use of data and violation of personal privacy, destruction and/or modification of civil registry data without legal basis. Coupled with a lack of human, material and administrative resources, civil registry is thus limited in both its recording capacity and its relevance, since it is presumed to be fallible. To illustrate this point, Senegal's civil registry is administered by volunteer or contract agents (around 50%) whose knowledge and training in administrative procedures are regularly incomplete and sometimes deficient[139] . The progressive digitization of civil registries throughout the world remains highly heterogeneous today, despite a genuine international commitment to legal and IT standardization and harmonization[140] . Relatively complex for the reasons outlined above, many developing countries are implementing digital civil status projects that do little or nothing to comply with the best practices of developed countries, mainly due to a lack of IT resources. In addition to these structural problems, there are also organizational issues, such as the lack of communication between certain ministries, institutions and organizations, which are developing separate projects with the same objective: to develop a reliable digital civil registry.

"UNICEF insists on the need to include birth registration and the issuing of an associated certificate in all projects concerning civil status. France must defend the same position as UNICEF"[141] . *It is* also worth mentioning the cultural and social discrimination that stands in stark contrast to the right to family identity[142] . In concrete terms, gender inequality exists in certain countries, and in a pronounced way, to the disadvantage of women and, by extension, their children. Sometimes, only men have the legal capacity to declare their children[143] . The result of these cultural traits, which developed countries have also experienced, is inevitable: lacking financial resources and time, most of these men fail to register their children's births, which often leads to their children having only a common name. In practice, as soon as two parents have the same legal capacity, the probability of registration increases significantly. Finally, it should be pointed out that in the event of the father's absence, contestation of paternity or death, women represent the only chance for a child to be declared in order to obtain a legal existence. In a way, the cultural customs of certain countries accentuate and aggravate their lack of identification. Since 2019, UNICEF has been advocating five measures

[139] FOUQUET Kevin, "L'état civil sénégalais aujourd'hui de l'enregistrement à l'archivage, les difficultés d'un outil de bonne gouvernance et de respect des droits humains", "(...) moreover, only 14% of the agents are civil servants. The rest are either contractual (50%) or voluntary. Staff are therefore in a precarious situation, knowing that their remuneration is low, and that their situation is inevitably becoming more precarious...", June 11, 2020, consulted online, p.77.

[140] "Les 'CNIL' mondiales prennent position sur les grands débats internationaux en matière de protection des données personnelles CNIL", accessed on November 12, 2021 at

[141] National Assembly report. *op. cit*. Available at the following address

[142] The widest possible protection and assistance should be accorded to the family, which is the natural and fundamental group unit of society, particularly for its formation and as long as it is responsible for the maintenance and education of dependent children. Marriage must be entered into with the free consent of the intending spouses, Art. 10, OHCHR | International Covenant on Civil and Political Rights, consulted online May 3, 2021.

[143] In Indonesia, single mothers or mothers without a marriage certificate are not allowed to register their child and parentage with the civil registry. Similarly, Bhutan's civil registry does not recognize children of unknown fathers.

particularly relevant to providing and protecting children's right to an identity from birth: "*1. Issue a birth certificate* [or rather proof of identity] *to every child from birth. 2. Give all parents, regardless of gender, the means to register their children at birth. 3. Link birth registration to social services. 4. invest in secure, innovative technological solutions to facilitate birth registration. 5. encourage communities to require birth registration for every child. In* light of these findings on the importance of identity and the rights of children, and consequently of adults, it is hypothesized that certain IT features of blockchain technologies could represent a major technical tool in the service of a digital identity that is accessible and legally recognized by all.

1.1.3.2 Natural law, identity claims and universal identity

Natural law is rooted in human nature. It is rooted in the natural behavior of people, in their supposedly innate instinct to respect other people, who are also subject to this natural law. It is deemed universally valid and applicable to all people, whatever their place or time. In legal terms, natural law is a "*rule considered to conform to* [man's] *nature and as such recognized as ideal law*"[144] . More simply, natural law is a form of legal feeling, latent or expressed, which is said to be rooted in the very depths of humanity. Unlike positive law, which evolves and sanctions according to the evolution of social mores, natural law is fixed. According to the English philosopher John Locke, positive law and natural law are not opposites, but rather cumulative. Natural law, according to Locke, is universal and transcends laws enacted by governments. It is founded on the principles of reason and natural justice, and is applicable to all human beings. For Locke, individuals have natural rights such as life, liberty and property, which predate the existence of the state, and which the state must protect. For him, the natural origin of all Man is to be in essence in "(...) *a state of perfect liberty, a state in which, without asking permission of any man, and without depending on the will of any other man, they may do what they please, and dispose of what they possess and of their persons, as they think fit, provided they keep within the bounds of the law of Nature*"[145] . In short, John Locke defended the idea that natural law is superior to positive law, and that the latter must be in conformity with natural law to be morally just. In his view, government is bound to protect the natural rights of individuals and respect their individual liberties, even if this means limiting its own power. Studying the foundations of Web 3.0

[144] CORNU Gérard, "Vocabulaire juridique", in Association Capitant, 8th ed. 2007, PUF coll. Quadrige.
[145] LOCKE John, "Traité du gouvernement civil", 1690, French translation by David Mazel in 1795 from the 5e London edition of 1725, p.17, available at

leads us to assume that these foundations of natural law are in line with the idea that a cryptographic law self-regulated by online communities would be superior to positive law.

Universal principles have long been enshrined in domestic law, by virtue of Article 1 of the 1789 Declaration of the Rights of Man and of the Citizen, which states: "*Men are born and remain free and equal in rights. Social distinctions can only be based on common utility*"[146] . The universal and unalterable nature of natural law can also be linked to the desire to ensure a universal right to identity for all individuals. This idea of the universality of identity was already expressed by French academician Amin Maalouf before the growth of the 1.0 digital era: "*By successive regional groupings* [via the Internet]*, humanity would one day reach the supreme gathering* [a universal identity]"[147] . According to the academician, "*The basic postulate of universality is to consider that there are rights inherent in the dignity of the human person* [i.e. that everyone should be able to live with honor and decency]". In practice, to achieve such a universally attributed and claimed identity on a planetary scale, several questions arise, namely how to create a global source of (digital) identity that everyone can trust, but which is neither owned nor controlled by any particular company or government? Are we experiencing an identity war, or simply political demands due to digitally-enabled freedom of expression? How can we ensure that the emphasis on identities does not lead to the radicalization of debates, i.e. a form of fragmentation of civil society? Etymologically, the universal is that which "*extends to the whole earth*"[148] , i.e. to every person. According to the Larousse dictionary, it is possible to attribute several meanings to the term "universal"[149] . However, for the purposes of our research, we will consider the following meanings: "*that embraces the totality of beings and things: a universal value*"; "*that has the character of universality*" and "*that which is universal: to rise from the particular to the universal*". The universal is in principle that which takes into consideration and includes all cases without exception. The universalism of identity represents identity with regard to the whole of humanity, i.e. the very fact of existing and having an identity.

Now that we've distinguished a few concepts, we need to take a closer look at the notion of technological universality, which in this research refers to the universal nature of digital identity. In the online world, the concept of universality refers to the accessibility and openness of information systems, in principle without borders or distinctions for Internet users. Some legal experts are pioneers, and have understood that t h e universal aspect of digital identity is a necessity.

---

[146] Declaration of the Rights of Man and of the Citizen of 1789. Conseil constitutionnel. Accessed on September 5, 2022 at the following address

[147] MAALOUF Amin*, op. cit. "*Les identités meurtrières", "[...] the new means of communication offer a very large number of our contemporaries, people who live in all countries and are bearers of all cultural traditions, the possibility of contributing to the elaboration of what will tomorrow become our common culture", p.112 and pp.147-189.

[148] Etymology of universal. cnrtl.fr. Available at the following address

[149] Larousse. Definitions, in *Dictionnaire de français Larousse*, consulted on September 5, 2022 at the following address

A legally enforceable, supranational identity guaranteeing total protection of personal data is an absolute necessity, and one that the digital industry can no longer avoid"[150] . A universal digital identity would consist, by its very existence, in affirming online our membership of human civilization. Such a possibility would enable anyone to join a digital humanity made up of simple, verified individual existences. This proof of digital existence would also open the door to the recognition of associated rights, depending on the IT functionalities and limits that such a system would imply. A universal digital identity should enable people to claim their singularity and some of their belongings, since uniformity prevents any singular identity. Academician Amin Maalouf asks whether we should welcome the fact that people are becoming increasingly similar[151] . On the one hand, the standardization of human beings can lead to and facilitate a universal identity, but on the other, it can also contribute to the destruction of cultural diversity. In this way, the promotion of online identities does not threaten the universality of a decentralized digital identity, as we discuss below, but rather strengthens it through diversity. With a digital identity that is by design open and interoperable, every individual can join a form of universal online identity, within which he or she can claim some of his or her identity parcels and belongings.

However, an important distinction must be made between a universal digital identity system and a universal digital identity proof system. The former is intended to serve as a common identification and authentication system for all natural persons, while the latter's more specific vocation is to serve as a foundation and digital gateway for other traditional identity systems (civil status, digital identity 2.0, for example). A universal identity system is therefore broader and more utopian than a universal proof-of-identity system, whose aim is to perfect existing identity systems. The decentralized digital identity (IND) studied below represents a new technical foundation for John Locke's social contract. With an IND, legislative power remains in the hands of identity providers, while executive power is transferred to the Internet users who control it. Blockchain technologies could be used as an open data registry, enabling certain identity information to be anchored immutably and decentralized on the Internet[152] . In other words, setting up a universal, decentralized system of proof of identity makes it possible to some extent to move towards a digital identity, thanks to the reappropriation of digital behaviors and identities by Internet users. In this respect, the World Economic Forum (

[150] BENSOUSSAN Alain, *op. cit*, "L'identité numérique 5.0", p.47.
[151] MAALOUF Amin, "Faut-il vraiment se réjouir de voir les hommes de plus en plus semblables?", *op. cit.* in "Les identités meurtrières", p.120.
[152] De FILIPPI Primavera, "Blockchain and the law", "Over time, blockchains could anchor new public infrastructures and even potentially global and transnational systems, accessible to anyone with an Internet connection", in *Harvard University Press*. Location 109 of 7004.

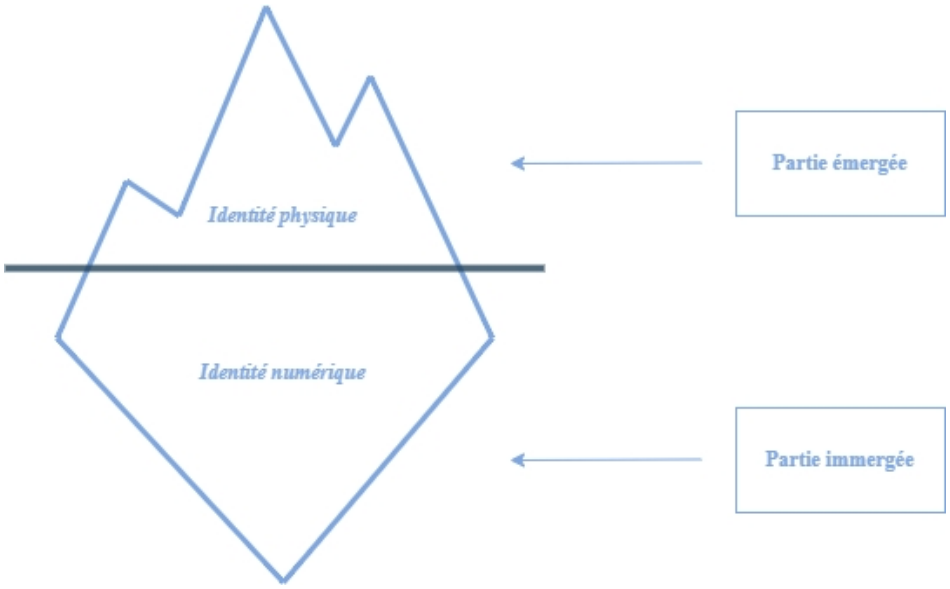
Forum - WEF") proposes to demonstrate the ubiquity and importance of digital identity for people's rights, highlighting the necessary use of new technologies such as blockchains[153] . It seems that in this modern, digital society, people are becoming more aware of their identity allegiances, perhaps more so than ever before. Blockchain technology and decentralized digital identity are enabling new forms of online expression whose vocation is to be as universal as possible. Achieving a universal digital identity through 3.0 technologies, such as a self-sovereign digital identity, however, presupposes the uniqueness and enforceability of one's digital identity against third parties. For these conditions to be met, each individual must be both the issuer and the maker of his or her own proof of identity. While, in theory, self-sovereign digital identity ensures this, in practice it turns out that a sovereign trusted third party (regalian administration) remains almost systematically required for the issuance of identifiers and proofs of primary (civil) and sometimes even secondary (extended) digital identity. Consequently, the right to universal digital proof of existence is desirable[154] and technically possible using the new IT concept of decentralized identity, which is already gaining momentum thanks to the new blockchain technologies. Finally, a system of universal proof of digital existence seems to be essential, thanks to the new technico-social concept of a decentralized digital identity[155] recognized, interoperable, secure and industrializable.

[153] According to our study, decentralized digital identity (IND) could be added to this scheme published by the World Economic Forum. Strategic Intelligence | World Economic Forum. Accessed online March 02, 2023.

[154] In every age, there have been people who have considered that there is a single major affiliation, so superior to the others in all circumstances that it can legitimately be called 'identity'. For some, it was the nation, for others religion or class. But it's enough to look at the various conflicts [of the 19th century] to realize that no single affiliation prevails in an absolute manner, *op. cit.* Amin Maalouf, in "*Les identités meurtrières*", p.19.

[155] Throughout this thesis, we consider that the term *hybrid digital identity* refers to a 2.0 and/or 3.0 digital identity derived from a physical identity materialized by an identity document. A *hybrid digital identity* is thus a *digital identity derived from* a physical, civil and legal identity document. V. Glossary.

1.2 Exploring the concept of iceberg identity



If identity were an iceberg, its emerged part would constitute its primary, root, objective identity, i.e. its legal identity, as suggested in the previous sections. Its submerged part would represent its secondary, subjective, i.e. extended, identity. From a global perspective, these two parts form a single whole, a global identity. It is also possible to focus on one or other of these parts (emerged/immerged), depending on the observations of each individual. This iceberg can in fact be analyzed in as many distinct ways as there are different observers to describe it. Depending on its (adjustable) waterline, its emerged part may appear more important than its submerged part, and vice versa. Taking this concept to its logical conclusion, if each Iceberg (analogy for a person) is unique in its characteristics, and moves differently depending on the oceans it sails on (analogies for cultures and societies), the identity of each Human being would be comparable to an iceberg drifting on the different oceans that make up humanity. This analogy underlines the possibility of adopting a relativistic, global conception of identity. The external part represents who we are in the eyes of society, i.e. the part of our being exposed to sociality and reflecting a social and external image of identity. The internal part constitutes our subjective and psychological identity, strongly influenced by (and sometimes even in conflict and contradiction with) the external part of identity. The waterline is assumed to be specific to each relationship between its emerged and submerged parts, i.e. between physical and digital identity. To sum up with this analogy, these two parts coexist for the same person, because an iceberg continually transforms according to its environment, thus consecrating the complexity of the very concept of identity. This study highlights three major elements

of people's identity in the digital age, namely their physical, civil and psychosocial identities. We suggest that these elements are cumulative, depending on the contexts of the global identity they characterize.

Chapter 2: Chronology of a redefinition of identity in the digital age

Before tracing a partial chronology of the history of computing and its legal considerations, from Internet 1.0 to Internet 2.0 and then 3.0, two fundamental considerations on the relationship between Man and computing need to be recalled. Firstly, computing is binary. When a computer applies a model, social negotiation is no longer possible. Negotiation is always possible between two people, but not between two machines. Negotiation, echoing the notion of consent, is not a process implemented online by default; it has to be designed and programmed. In this way, the computer becomes fatal, since it cannot negotiate what is real, unlike man. This is often the case when an online service fails to meet the needs of an Internet user, such as a simple omission of a checkbox or the impossibility of contacting a service by telephone, resulting in delays in processing the request. While IT is inevitable for access to certain online public services, it is not for the secondary digital identity of Internet users, which is negotiated more freely online with social networks. While 3.0 technologies do not escape these principles of binarity and non-negotiation, it would nevertheless seem that they can contribute to making certain identity management processes more transparent and open, i.e. partially negotiated. Secondly, the idea that any file is bad treatment for human beings should never be underestimated. The act of creating a file, whether physical or digital, involves establishing a relationship not between human beings, but between a human being and an object. This means that the management of objects can sometimes reach such a level that the humanity of individuals is erased. In other words, and in addition to the previous point, social relations are masked by the interaction between man and machine. The creation of a file introduces the possibility of maltreatment through reification, i.e. the transformation of a human subject into a computer object or identifier to which physical or computer processing is applied, which may in some cases be contrary to legal or moral rules. This principle applies to all files without exception, and summarizing people's lives in files necessarily implies a risk of possible mistreatment. For example, if a judge were to judge cases solely on the basis of facts taken from computer files, and without the presumed guilty party being able to express his or her views, then his or her judgment would be dehumanized and likely to be a source of abuse. 3.0 technologies and their applications may also represent a risk, as these more or less decentralized technologies offer the possibility of storing files such as identifiers and digital interactions of Internet users immutably on decentralized infrastructures, such as

public blockchains, making it impossible to modify or delete. In view of this, it is suggested that personal data should not be considered as a matter of commercial law, but certainly of personal law. Personal data is an integral part of people's identities, which means that the commoditization of such data is undesirable, even if it is already possible with Web 3.0.

2.1 The origins of the Internet (Web 1.0)

In 1969, the Internet's forerunner, Arpanet for "Advanced Research Projects Agency Network", was a military project designed to address strategic communications issues on a US scale. The initial aim of the project was to catch up with the technological advances of the Soviet Union[156] . However, the "World Wide Web - *www*", Internet[157] , quickly outgrew the initial idea of its designers, whose main founder was the famous British computer scientist Tim Berners-Lee[158] , before being taken up by the scientific and academic community[159] . This academic and scientific work has had a major influence on the Internet's infrastructure, with the progressive questioning of its neutrality[160] . While the Internet was able to develop thanks to funding from the US military, its expansion also stemmed from the original ideology of its engineering community, for whom respect and protection of online rights and freedoms were fundamental[161] . From the outset, the social dimension of the project has been a major one, since all its technical advances are the result of the ideologies and multiple communities that have made the Internet what it is today. So, before being a territory, the Internet is a social movement[162] , an observation also shared by the Web 3.0 revolution, of which it is a part. From the official launch of the Internet on January 1er 1989, with the advent of the hypertext link and the NCSA MOSAIC[163] browser, the Internet has gradually spread across the globe.

---

[156] On October 4, 1957, the Soviets launched the first artificial satellite in history, named "*Sputnik*".
[157] Derived from "*network*" and loosely translated as "*inter*" followed by "*net*", for "*network*". Refers to a global telecommunications network linking computers or local networks, enabling the transmission of data of various kinds (electronic messages, text, images, sound).
[158] Timothy John Berners-Lee is an English computer scientist best known as the inventor of the *World Wide Web*. He is Professor of Computer Science at Oxford University and Professor at the Massachusetts Institute of Technology. On August 6, 1991, he put the very first website online, outlining the first operating instructions for the Web and giving access to its source code, i.e. the heart of the Internet, so that every user could retrieve it and contribute to its expansion: Timothy John Berners-Lee had just offered the Internet to mankind, and we see that Satoshi Nakamoto did the same for the Bitcoin protocol. The point of convergence between these two enigmatic characters is thus characterized by their humanism and financial disinterestedness.
[159] History was made on October 29, 1969, when two computers (at UCLA and Stanford) connected for the first time by satellite communication, making these two institutions of higher learning the first hosts of what would later become (on August 6, 1991, when Tim Berners-Lee announced the creation of the *World Wide Web* Internet.
[160] This is the principle of equality and treatment (non-discrimination) of all data flows on the Internet.
[161] Freedom of access and near-freedom of use are at the root of the Internet, which in fact responds to a need for sociability.
[162] "Internet History of 1980s | Internet History | Computer History Museum", accessed online January 13, 2022; In 1985, the Internet counted around 2,000 users/hosts, *v.* PARACHINI A. "30 ans du web : les grandes dates de l'histoire d'internet", in *Le Quotidien*, 2019, available at
[163] Wikipedia, the free encyclopedia, *Mosaic (web browser)*, accessed July 27, 2021.

to become what this research refers to as Internet 1.0 or Web 1.0 (~1990- 2005)[164] . Next comes Internet 2.0 (~2005-2020), with the emergence of networks, i.e. the first online communities, blogs and social networks. By 2022, nearly 4.9 billion[165] Internet users will be consuming online content on a daily basis on websites such as Facebook, Amazon and Google, to name the most famous.

Since the origins of Web 1.0, Internet 2.0 has become more immersive, more consumerist, with Internet users finding everything they need almost instantaneously. They become potential customers looking to satisfy their own real or latent desires. This phenomenon of commercializing data and digital identities on the Internet began in the mid-1990s, due to a predominantly dual market structure involving Internet users and professionals. These two categories - today non-exclusive - operate as follows: the user is the subject of a massive collection of personal data in exchange for access to service providers who generate advertising revenues indexed to the profiling of individuals and their collected data. In other words, the Internet has no longer simply become a means of accessing knowledge, but an end enabling users to escape a certain social reality[166] . At this point, it seems impossible to approach the subject of 3.0 technologies without understanding the importance and impact of 2.0 technologies, which refer as much to the concept of digital identity as to online social networks. A few decades later, these development practices have led to a gradual and accepted centralization of the Internet, directly operated by operating and service providers, the GAFAM and BHATX[167] holding and operating servers to the point of exceeding certain limits in terms of data protection and individual freedoms. This IT centralization has gone hand in hand with legal centralization, as jurist and doctor of law Primavera De Filippi explains: "*although the original conception of the Internet was to decentralize power and encourage freedom of communication - even at the expense of spam, fraud and crime - over the last decade it has become increasingly concentrated and regulated*"[168] . In its new strategy published in 2021, the European Commission insists that

[164] Also known as "*read only web",* because the user reads only the information on the website. This unidirectional scheme limited interaction between web users, as it was not very ergonomic, accessible or intuitive. Web 1.0 enables the simple reading of online data, Web 2.0 the reading and writing of online data and Web 3.0 the reading, writing and ownership of online data, the latter being a combination of Web 1.0's original desire for decentralization and community governance with Web 2.0's modern interaction functionalities.
[165] PATARD Alexandra, January 26, 2022, "30 chiffres sur l'usage d'Internet, des réseaux sociaux et du mobile en 2022", in *BDM*, available at
[166] Witness the growing phenomena of cyberstalking and social isolation in Japan (the "*Hikikomori*").
[167] GAFAM is the acronym for the five largest American Web companies -Google, Apple, Facebook, Amazon and Microsoft - which dominate the global digital market while offering digital identification systems to their users. BHATX stands for Baidu, Huawei, Alibaba, Tencent, Xiaomi, the five largest Chinese technology companies.
[168] De FILIPPI Primavera, "Blockchain and the Law," in *Harvard University Press*. Location 189 of 7004.

on the importance of establishing a new digital trust[169] . Gradually, recommendation and targeting algorithms[170] are exerting an ever-increasing influence, contributing to a form of unconscious enclosure of the user in a personalized bubble of which he or she is no longer master. Internet users are reduced to a kind of available brain time, with little capacity to understand how their data is managed behind the scenes of the "Big Tech" IT architectures that they constantly call upon. How much data is collected? For what purposes? For what purposes? What impact does it have on individuals and their personal and collective identity?

As former European Commission Vice-President Margrethe Vestager pointed out, "*when recommendation systems choose which information to promote and which to hide, they profoundly affect what we know about the world.* (...) *The world we see through these platforms seems so real that it can be hard to remember that it is actually constructed through the choices algorithms make about what we should see*"[171] . Other adjacent drifts, such as mass surveillance, risks of personal data leaks or censorship, have come to light. By way of illustration, according to a report by the Pew Research Center[172] , the majority of American adults get their information from Facebook and Google, which have become the unofficial gatekeepers of information in the United States and many other countries around the world. Like any digital revolution, and after a while, legislators tried to regulate Internet activities, but this new digital era is overturning the previously established legal order: "*The Internet marked the beginning of a new paradigm for regulation - one in which regulation would be enforced through the rule of code* (...). *Governments extended their control by requiring intermediaries to modify their code to maintain and comply with the laws of their jurisdiction*"[173] . In addition to the fact that the Internet was born without a native identification system for individuals, i.e. with a missing [technological] link[174] , it is also undergoing an identity crisis. Indeed, it has strayed from the utopia initially imagined by the World Wide Web as a space of unprecedented freedom, enabling users to share information without borders, without surveillance, and without censorship. This technological concentration, whose innovation is today owned and patented by a minority

[169] "A true digital transformation must start from the fact that European citizens and businesses have confidence in the security of their applications and products. The more interconnected we are, the more vulnerable we are to malicious cyber activity. (...) Feeling secure is not just a question of cyber security. Citizens must be able to trust the technology itself", Communication Shaping Europe Digital Future, in *EU-Lex*, consulted online December 6, 2021, p.4.
[170] Increasingly powerful algorithms now determine which images, videos, music, messages or reading material we consume.
[171] RTBF info, "Des algorithmes plus transparents : l'UE va les réclamer à Facebook et Google", published on October 30, 2020, accessed online on July 27, 2021.
[172] "10 facts about Americans and Facebook 2021", in *Pew research Center,* accessed online July 27, 2021.
[173] De FILIPPI Primavera, *op. cit*. Location 4028 on 7004.
[174] CAMERON Kim, "The laws of identity on the Blockchain," in *Keynote at the European Identity & Cloud Conference.* 2018, available online

of companies in an oligopolistic situation, to the detriment of Internet users and a free Internet, which in reality is no more than a shadow of its original philosophy and conception. These major technology companies are gradually establishing a form of digital monopoly, i.e., a technico-political system undergoing constant technological change, the operation of which they alone can control. To illustrate this point within Web 2.0, there is only one digital object that an Internet user can own and hold on the Internet: a domain name[175] . But with Web 3.0, Internet users can theoretically appropriate entire facets of the Internet to assert their online rights, as well as new behaviors or digital possessions (digital tokens of the "NFT" type)[176] which are discussed later in this study. Today, we need to see the emergence of a fairer Internet, more respectful of Internet users, over whom they should have control. The emergence of a decentralized Web 3.0, based on blockchain technologies and decentralized digital identities, seems to be in line with the original values of the Internet's founding fathers.

2.2 Defining digital identity

The term digital identity is often complex to define. To provide a comprehensible reality, it can be systematically linked to its origin: physical identity. Digital identity would thus be "a *process that enables identity elements to be transcribed onto a digital medium, which in turn enables legal identity to be traced*"[177] . Generically, digital identity can be defined as all the forms of presence and traces that an Internet user generates when browsing online. According to this definition, digital identity represents an extension of a person's civil and social identity within the digital space. A digital identity would then be no more than a multitude of online copies of the same administrative, physical identity. The borderless, instantaneous nature of the digital environment enables people to express their psychological and social dimensions in a new way, far removed from the traditional, regal form of identity. Thus, it seems that citizens a r e gradually benefiting from a

[175] Each domain name is unique and cannot be duplicated. While websites can be duplicated, this is not possible for domain names, which introduces and historically represents on the Internet a first notion of ownership and digital scarcity (bitcoins being the second).

[176] V. Next parts. In theory, this right of ownership over digital elements is possible thanks to certain technological applications such as "Non Fungible Tokens" (NFT), which generate a unique and non-duplicable title of ownership thanks to its traceability on a public blockchain. While some legal experts claim that NFTs are pure speculation or a scam, it should not be forgotten that, in Web 2.0, many Internet users publish their intellectual works to the world in return for a form of digital social recognition, i.e. support through likes, shares, etc. It is therefore undeniable that NFTs are a form of property that can be duplicated. It is therefore undeniable that NFTs open up new possibilities for Internet users in terms of both ownership and digital patrimonialization. The UK High Court has ruled in favor of NFTs being considered as property, and that victims of NFT theft can take action to have their stolen assets frozen by court order. GEE Kate, MARSHALL Alasdair, "NFT's recognized as property", April 20, 2022. Accessed May 2, 2022, at

[177] COUTOR Sophie, FAHER Mourad, HENNEBERT Christine, Rapport du Ministère de l'Intérieur, octobre 2020 v.1.0, "Blockchain and digital identification, BCID, restitution des ateliers du groupe de travail du 8 juillet 2020 sur l'identité numérique," accessed online August 9, 2021, p.31.

rediscover their initially static, physical identity dynamically and online. The aim is to determine the perimeter of digital identity in terms of its current and future social and technological uses. While online a person is first and foremost represented by identifiers, i.e. by his or her browsing and sometimes digital habits, it seems that a legal identity is not systematically required to access certain digital services[178] . The scientific literature mainly defines digital identity in its practical aspects through computer elements belonging to Web 2.0 or Web 3.0. In his book Ego 2.0[179] , Pascal Lardellier, Professor of Information and Communication Sciences, enshrines digital identitý as a relationship to others. He highlights the development of the ego with 2.0, which forms a "*digital expressive I*". This Ego 2.0 would thus develop within digital social networks with the possibility of expressing oneself and putting oneself forward in the digital and social sphere. For his part, Dominique Cardon[180] , Professor of Sociology, believes that digital identity is "*less an unveiling than a projection of the self*". Further down the identity chain, Fanny Georges, a semiologist and lecturer in information and communication sciences at the Université Sorbonne Nouvelle, considers that "*identity is becoming mixed, made up of information acquired face-to-face and on social sites*"[181] . At the heart of Internet culture, digital identity was historically synonymous with distancing and anonymity between a person's civil identity and their online avatar - a digital alter ego. The Internet enabled individuals to create different identities for themselves, freeing them from bodily determination. Digital identity has thus become a new form of self-expression, whether pseudonymous or assumed. The complementary - but by no means exhaustive - portraits evoked by these authors are more topical today than ever before, since the mixed, objective and subjective digital identity is necessarily that which emerges from interactions with information systems. It is therefore possible to distinguish two main categories of digital identity, linked to the first definitions of identity:

(i) *Root* or *primary* digital identity, which represents the extension of our physical and legal identity into the virtual world. This first category includes a person's civil identity, which they present online to prove that they are who they say they are. Thus, the root digital identity simply represents an extension of the legal identity based on identity papers and the subjective identity based on pseudonyms,

---

[178] SENAT, Report no. 432 (2010-2011), submitted on April 13, 2011, Proposition de loi relative à la protection de l'identité, 1er June 2022, "Most transactions carried out online do not require precise identification of the buyer: payment is sufficient", available at the following address. This proposal was adopted on March 27, 2012 by law no. 2012-410, available online at

[179] LARDELLIER Pascal, BRYON-PORTET Céline, "2.0, quelques considérations théoriques sur l'identité et les relations à l'ère des réseaux", in *Les cahiers du numérique*, 2010, Vol. 6, consulted online September 15, 2021, p. 13.

[180] CARDON Dominique, "L'identité comme stratégie relationnelle", in *Hermès*, revue 2009, n° 53 consulted online on September 15, 2021.

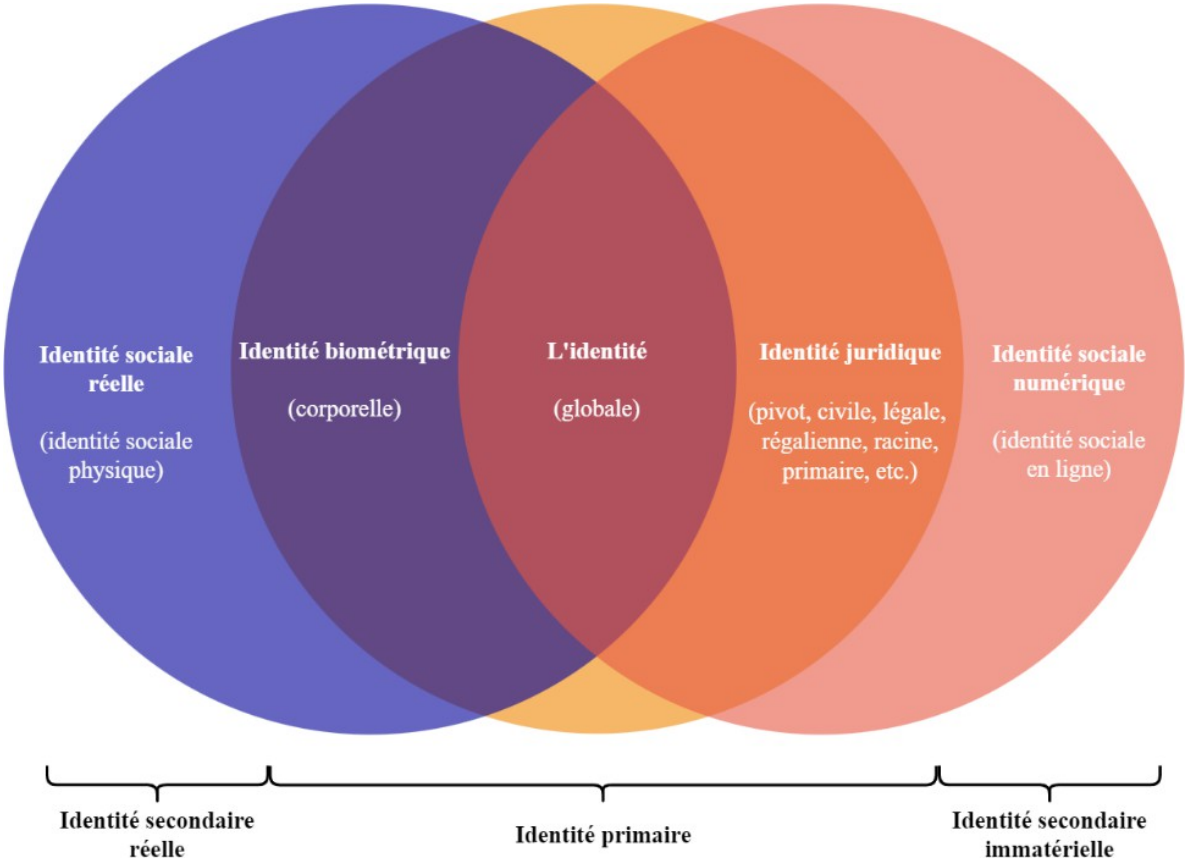
[181] GEORGES Fanny, "Représentation de soi et identité numérique : une approche sémiotique et quantitative de l'emprise culturelle du web 2.0" in *Réseaux*, 2009, n°154, consulted online September 15, 2021, *see* also "Eternités numériques : la communauté numérique et la mort", 2020, pp.69-88.

e-mail addresses and telephone numbers when browsing online services. This primary identity, projected into the digital world, is generally only used for certain specific and repetitive administrative or legal acts, in order to reliably identify Internet users when accessing an online public service via FranceConnect, for example[182] . In principle, a person's civil identity is stable, i.e. it remains legally unchanged whether it is attested via a physical medium (paper, plastic), or electronically with a login and password. The majority of an Internet user's digital interactions stem from a second type of digital identity, extended and prolonged from the first.

(ii) *Extended* or *secondary* digital identity. This considers all the secondary digital identity traces that an Internet user generates on online services. This second category includes our social network pseudonyms and profiles, our video game avatars and other online accounts of a commercial (Amazon, Pinterest, Leboncoin) and interactive (Signal messaging, Telegram) nature. These extensive traces of virtual identity are created by Internet users, who decide how to set up their accounts and choose their pseudonyms or quasi-names. A certain freedom of use and management is thus possible thanks to pseudo-anonymity, in relative opposition to the root digital identity fixed by law as previously mentioned. In the event of problems with this secondary identity, it seems that only proof of the primary identity can identify the person in question (in the event of loss of access or identity theft). However, there are exceptions, still marginal, within the digital universe in which a secondary identity can be created without a trusted third party, by substituting itself for a primary identity. This is the case of Metavers and self-sovereign identity (INAS), which will be studied in later sections.

[182] *FranceConnect* is an online identification and authentication solution proposed by the French government to secure and simplify connection to over 900 digital services to date (2022).

To summarize these remarks and enrich the iceberg concept of identity introduced earlier, it is possible to summarize the facets that coexist for each global identity in a series of several concentric circles:



Many authors and experts perceive the Internet as a mere virtual extension of the real world, while others see it above all as a borderless space of freedom in which pseudo-anonymity (discussed below) is established as a fundamental right. While the categories illustrated are purely indicative, they nevertheless reflect two visions that may be complementary or different, depending on each individual's perception. In the light of these two apparent positions, it seems that the more the technologies studied become intertwined, the more people's secondary identity attempts to free itself from the primary identity assigned by the state. We suggest that this desire to liberalize digital identity is necessary, and perhaps utopian for some Internet users. Today, a teenager's digital identity is born long before his or her legal capacity[183] . This temporal gap between digital behaviors that are in principle impossible for young teenagers is particularly significant on social networks, where they are by nature less informed and more susceptible to influence than adults. In this respect, decentralized digital identities can help to reduce the gap between legal responsibility and these young people.

[183] By way of illustration, many teenagers create their first digital traces on social networks as early as 13 or 14 years of age, producing legal effects (buying and selling video games, asserting their identity, etc.) even though their legal capacity doesn't exist until they come of age.

socio-numerical practices that disrupt the effectiveness of legal rules[184] . When surfing the Internet, the two aforementioned categories of digital identity are used in a complementary and more or less mutually exclusive way, depending on the purpose of the services provided to the user. In terms of use, primary and secondary digital identities are intended to authenticate users wishing to access online services. However, secondary digital identities have an additional dimension, that of freedom of choice regarding the online presence a web user wishes to assume. The concept of digital identity raises many questions about systems for managing, identifying and authenticating people's online identities: why isn't digital identity unique and universal? Why can't an individual be recognized by his or her digital alter ego as simply as in the physical world? What level of transparency and trust do Internet users have online? How can we guarantee the authenticity of their identities and the application of their fundamental rights online? Does the state have the capacity to position itself as a digital identity provider? Is it possible for the private sector to intervene to dematerialize our identities, and what kind of protection framework is needed for personal data?

For some specialists, a double catalyst is at work within the digital sphere, reinforcing the conceptualization of a primary and secondary digital identity, as French communication and information scientist Olivier Ertzscheid reminds us: "*upstream, it contributes to feeding the great reservoir of global identity; downstream, it offers many new opportunities to draw on the reservoir of available data to forge contextual identities*"[185] . As the physical and virtual worlds gradually merge, this upstream/downstream interdependence between identity and its evolution in digital space redefines the traditional meaning of identity, and tends towards a new form of identity, the *phygital* identity, already mentioned. According to lawyer Alain Bensoussan, a digital identity, whether attributed to a legal entity, a physical person or even a digital object, necessarily implies the combination of three elements: a third party's acknowledgement of the birth or creation of a singular entity, the attribution of one or more unique identifiers, and the registration of these identifiers in a centralized or decentralized digital register, as the case may be. These three elements make it possible to characterize simply and impersonally whether a digital identity is characterized or not. However, it should be emphasized that registration is carried out using a password, a unique secret code, recorded in encrypted form by online services and all too often reused, i.e. shared between various online services[186] , which increases the risk of fraud.

---

[184] ADAM Louis, "Accès des mineurs aux sites pornographiques : qu'est-ce que la vérification d'âge en 'double anonymat'", Published February 17, 2023, in *Le Monde*, online at

[185] ERTZSCHEID Olivier, "Genèse: qu'est-ce que l'identité numérique?", Ed. *Open Press*, chap. 1, accessed online August 9, 2021.

[186] This secret is not only encrypted, but also widely shared when users use the same passwords for different online services (which increases the risk of the secret being revealed in the event of a breach in one of the online services holding it). It should be noted that passwords are, in theory, systematically

the risk of identity theft or data breach. The process of creating a digital identity is, in fact, a particularly social and iterative one. This is emphasized by French sociologist Dominique Cardon in his essay "*The Design of Visibility*". Cardon identifies three elements of this process[187] : Internet users fragment and then deploy different segments of their digital identity according to the online services they use; an online identity can only be constructed in interaction with processes of denigration and social recognition; and the perception of a digital identity influences, by extension, a person's primary identity (in other words, a person's social life is regularly impacted by interactions with their digital identity). Although the search for uniqueness and singularity is one of the main motivations of Internet users, it has to be said that some of its facets remain largely subject to social and collective norms, such as mimicry or the search for sensationalism (Ego 2.0).

Since the rise of Web 2.0 and the proliferation of online services, it has become essential for European legislators to organize a body of legislation to regulate digital services and ensure the protection of European citizens. As a result, Europe has adopted a number of regulations, including the eIDAS Regulation[188] on electronic identification, authentication and trust services online, and the General Data Protection Regulation RGPD[189] , which are examined in the second section of this study and in the second part. As early as 2005, i.e. before the first personal data protection laws in Europe, the PIPL rules[190] in China or the CCPA rules[191] in the United States (California), Microsoft architect and digital identity engineer Kim Cameron, published the
"*seven laws of identity*"[192] . There is probably an unprecedented correlation between these seven principles and the foundations of data protection laws, from which the European legislator has drawn inspiration. Before identifying the legal qualification of the notion of digital identity in Community law, we need to distinguish between two terminologies suggested by specialist lawyers[193] , personal identification data versus personal data. Indeed, there are many different data flows, and just as many associated legal categories to account for them. Personal data

This means that passwords are still regularly stored in unencrypted databases.
[187] CARDON Dominique, "Le design de la visibilité", in *Réseaux*, n° 152, 2008, consulted online September 15, 2021, pp.93-137.
[188] Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, available at.
[189] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, available at.
[190] Personal Information Protection Law (PIPL) in China, equivalent to the European RGPD, coming into force on November 1er 2021.
[191] California Consumer Privacy Act (CCPA) which came into force in California on January 1er 2020, inspired by but rather far from the requirements of the RGPD.
[192] CAMERON Kim, "The Laws of Identity", "User control and consent; Minimal disclosure for limited use; Legitimate parties; Directed identity; Pluralism of operators and technologies; Human integration; and Consistent experience across contexts", in *identityblog.com* on May 11, 2005, accessed online on 10/28/2021.
[193] EYNARD Jessica et al. L'identité numérique; quelle définition pour quelle protection?", Ed. Larcier, 1ère edition 2020.

are not personal data, because they refer only to a person's civil identity, but also because they generally represent technical identifiers, such as biometrics. Personal data, on the other hand, involves an infinite amount of information that can be used to define the digital identity - civil or claimed - of an individual. It is therefore important to distinguish between these two forms of data, so as not to confuse them and to avoid confusing their respective legal frameworks with the eIDAS Regulation (personal identification data) and the RGPD (personal data), both of which are examined in detail in the following chapters. Notwithstanding its consecration by usage, it would be more accurate to substitute the term "digital identity" with "*electronic means of identification*". Some legal experts respond positively to this restrictive definition[194] , simply because the eIDAS Regulation studied in the second part of this study offers a precise definition of electronic identification "the *process of using personal identification data in electronic form uniquely representing a natural or legal person, or a natural person representing a legal person*"[195] . Similarly, authentication is "*an electronic process that confirms the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form*".

In a digital world where the collection of user data is essential to offer increasingly immersive and personalized online experiences, the application of the RGPD for its part can seem more complex in the face of this online commercial and behavioral reality. This situation presents both advantages and disadvantages. Indeed, in many cases, current digital identities do not comply with certain key principles of the RGPD. By way of illustration, it is common for online services to ask a web surfer for his or her date of birth in order to confirm that he or she has reached the age of majority. In this respect, there is no reason for this person to provide this personal data, as there are other equally effective and more privacy-friendly ways of proving their majority[196] . Other similar cases exist, due to convenience[197] and sometimes ignorance[198] . It seems that

[194] *Ibid*. "(...) as you can see, I've just abandoned the expression 'digital identity' for the first time", *op. cit.* p.6.
[195] Art. 3.1 of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions, *see* dedicated section.
[196] Proof of age is a particularly important issue, especially for minors under the age of 13. According to the Génération Numérique survey, 63% of them will have at least one account on a social network in 2021. Implementing a minimal and anonymous verification process for proof of majority requires the use of *ZKP* (see below) coupled with a decentralized identity close to a self-sovereign digital identity (INAS). Indeed, protecting adults from the massive harvesting of their ages by online services is a necessity that FranceConnect's federated identity solution does not meet at present (2021).
[197] For 60 years, password systems have been used, even though they are not optimal for Web 2.0 use. It was partly for this cybersecurity reason that smart cards were invented: to store passwords directly within the smart card, so that when the card is queried, a response is given without revealing the password. In reality, a PIN or similar password is sometimes required for this interrogation to provide additional security, but this is less restrictive than the simple use of a complex password.
[198] There are already various cryptographic methods that can be used to prove information with certainty without disclosing its content or source. In particular, the European Parliament will be referring to *Zero-Knowledge Proof (ZKP)* in 2019.

The digitization of people's identities mechanically multiplies the possibilities of harm to individuals, by multiplying the possibilities of malicious actors in the field of commercial espionage, identity theft or any other malicious act. The definition of a digital identity therefore depends on the context in which it is used, as well as the level of trust required to interact online: a relationship requiring a high level of trust requires access to the Internet user's primary identity, with the state acting as a trusted third party. Conversely, a relationship with a low or moderate level of trust is sufficient, in principle concerning the secondary attributes of the digital identity. Finally, a person's digital identity should be both constant over time, for certain essential uses (primary identity attributes), and temporary for other uses (secondary identity attributes). To this end, we'll see that decentralized identity represents an excellent way for this supposedly "augmented" digital identity to enable a person to decline his or her digital identity into as many digital identifiers as necessary. It allows users to designate each person by the function they perform within multiple digital communities[199] , while sovereignly managing[200] the lifecycle of each of these persons and their functions. As we will explain in the following sections, digital identity 2.0 certificates should not be confused with decentralized identity 3.0 certificates. While 2.0 digital certificates are now the basis of our digital identities, their multiplication can lead to a loss of control (by a third party or the person in question) over the identity of individuals. To this end, the 3.0 digital certificates (verifiable attestations) studied in the second part of this study make it possible to generate and share multiple digital certificates for the same person. Decentralized identity refers to a system in which individuals or organizations can have control over their own digital identity attributes, rather than relying on a centralized authority to manage and verify their identities. In this decentralized identity system, the identity of an individual or organization is stored in a more or less decentralized and secure database, using blockchain technology. In this way, each identity can be easily accessed and verified by others, thanks to cryptographic means.

[199] These are related to the various contexts and uses of a person's digital identity. In other words, each community (online services) must have its own *electronic registry* (be it a centralized server or a *blockchain, which is in* principle more decentralized). In this way, there is nothing to prevent a single person from having a multitude of digital identifiers in a multitude of electronic registers and their associated online communities.

[200] According to this principle, "(...) I must be able to keep the possibility of 'navigating' or 'expressing myself' in the digital world without being systematically identified: I remain free to use the identifier I wish, or not to use one", *op. cit. L'Identité numérique 5.0*. p.18.

2.2.1 Social networks and digital identity management models (Web 2.0)

With the emergence of the Internet, the need for Internet users to identify themselves has never ceased to grow. From the development of websites and social networks, to e-commerce and digital public services, several identity management models have followed one another, forming a Web 2.0 in the wake of Web 1.0. It appears that these digital identity management solutions are costly today: the global economy spent 4.93 billion USD in 2017 on identity verification[201] , without this figure including financial losses due to identity fraud, regulatory compliance obligations and costs, or IT security costs. The overall financial cost of establishing an online identification infrastructure is considerable. Indeed, this can lead to a reduction in the confidence of citizens and users in the management of their digital identity, while at the same time their requirements and needs in this area are constantly evolving. It is therefore possible to distinguish two main trends and models for digital identity: those in favor of a centralized digital identity versus those in favor of a decentralized identity. In both cases, provision and access can be broken down into a number of conceptual and technological variants, which this research explores in the following sections. Three generic schemes underlying any digital identity can be identified: the siloed digital identity model[202] , the federated digital identity[203] and finally a user-centric digital identity model[204] . Before discussing the technical differences and complementarities of these models in more detail, it is essential to offer a definition of two indispensable players in the digital identity market: the identity provider[205] and the service provider[206] . An identity provider is an organization, such as the French company IN Groupe[207] , which makes identity information available to users or online services. In other words, it handles the creation, maintenance and management of identity information on behalf of individuals or legal entities. To this end, it provides authentication services to service providers or stakeholders' IT applications. A service provider is an entity that provides one or more online services to individuals (websites, social networks). Some service providers are also identity providers (for example, when the creation of a user account and subsequent access to an online service are operated by the same entity). For the sake of simplicity, they are referred to generically, on the basis of the following principle

---

[201] "Global identity verification market size 2017-2027", translated from English, "From 2017 to 2027, global spending on the identity verification market is expected to grow by more than $13 billion, from $4.93 billion in 2017 to more than $18 billion in 2027", Statista online, accessed July 18, 2021.
[202] *Siloed identity.*
[203] *Federated identity.*
[204] *User-centric identity.*
[205] *Identity Provider.*
[206] *Service Provider.*
[207] IN Groupe, "Le Droit d'être soi, l'identité est un droit fondamental, IN Groupe contribue à le faire savoir", visit the website at the following address

if the service provider is also an identity provider, the entity in question will be referred to as an identity provider. Before the advent of digital social networks, social networks were purely physical, i.e. represented by numerous convivial places such as local restaurants or bistros. The revolution of digital networks lies in the fact that they transpose and reconnect online the diversity of these ecosystems, which were initially physical and independent. This rapprochement between physical ecosystems and digital social networks has highlighted a gap between them. While asserting segments of one's identity and diversity online seems to be a real step forward for society, confinement in a bubble of algorithmic recommendations or misuse of anonymity remain invisible but real dangers for Internet users (harassment, insults, identity theft). Researchers and authors Jean Lassègue and Antoine Garapon explain that "*digital technology, which provides individuals with possibilities that seem to be constantly renewed, could also close in on them like a trap*"[208] . Thus, what Pierre Bellanger wrote in 2004 seems to take on its full meaning: "*We need to regain our sovereignty over computer networks and systems, to regain control of our destiny. This is digital sovereignty*"[209] .

2.2.1.1 The impact of social networks on the construction of our identity

Social networks have become almost indispensable spaces for working, expressing one's personality, meeting people, getting information and learning. The list of uses is growing by the year, and these new digital spaces are already changing our physical behavior. The emergence of social networks has precipitated the advent of a new scientific discipline, the "*captology*" or the science of capturing our attention[210] . This quasi-science works with artificial intelligence (AI) algorithms focused on behavioral targeting of users. The more a user interacts with these algorithms, the more they can offer him or her content that will make him or her react, thus capturing his or her attention for as long as possible on these digital services. This race for attention capitalism, in which each user is progressively reduced to his or her available brain time, is not without consequences for people's subjective and secondary identities. In the near future, every social network will enable its users to create or implement digital avatars, a further step towards the concept of Metavers or a self-proclaimed state (see Liberland[211]), which are discussed later in this study. Digital social networks

[208] LASSEGUE Jean, GARAPON Antoine, "Justice digitale", in *PUF*, p.339.
[209] BELLANGER Pierre, "La souveraineté numérique", Ed. *Stock*, 2014.
[210] OSTOJIC Andréa, "La captologie ou l'influence par la technologie", 2017, in *Sciences Humaines*, accessed September 22, 2022, at.
[211] V. Appendix 4.

Do they characterize a form of new world order in which every Internet user more or less fictitiously and publicly stages his or her behavior and personal life?

In 2022, according to a study by[212] , the average Internet user will visit seven social networks every month, and in 2021, a survey estimates that French people will spend twelve hours a day on social networks[213] . While these figures need to be qualified in the face of the justification of the professional nature of a multitude of online activities, the fact remains that social networks have a psychological and social impact on the construction of people's identities. As early as 2016, a study asserted that the use of social networks collectively reduces attention span and can affect mental health[214] . In May 2017, the Royal Society for Public Health and the Young Health Movement published a report examining the positive and negative effects of social networks on young people's health. While they prove useful for society by promoting freedom of expression and freedom of information, they are paradoxically

"(...) *described as more addictive than cigarettes and alcohol (...) Rates of anxiety and depression among young people have increased by 70% over the past 25 years.*"[215] . According to two other studies published in 2019[216] and 2020[217] , the more hours a day a teenager spends on social networks, the greater the risk of depression and loss of self-confidence. Gradually, these trends seem to be confirmed. So, if the "deep self"[218] is systematically impacted by algorithms, could this be the ultimate goal of these applications? This is certainly the case from a commercial perspective, in order to avoid the risk of Internet users fleeing to other online services. So the answer to the question "*Do algorithms make us who we are?*" posed by author Aurélie Jean would be to say that they contribute a little more every day. For the younger generations, who make up a significant proportion of social network users, it seems that the latter have a proportionally greater effect on their identity construction than adults. If, as we've seen, our lived identity is dependent on social mimicry, then social networks exacerbate this effect on our identity (both physical and digital). In this respect, social networks encourage the demonstration of a biased, even false, lived identity, a phenomenon that leads to identity mimicry on the part of other users, who seek to behave identically, generating a social copying mechanism with sometimes devastating and more or less visible effects (social network addiction...),

---

[212] Facebook, Instagram, WhatsApp, YouTube, LinkedIn, Twitter, TikTok, in *Hootsuite Inc*. Retrieved September 21, 2022, from.

[213] ASNAV, " L'ensemble de la population estime à plus de 12 h 00 le temps quotidien passé majoritairement sur l'ordinateur et la télévision ", " Le 16ème baromètre de la santé visuelle démontre un fort impact des confinements sur la vue des Français ", cmavue.org. Available at the following address, p.1.

[214] HAYLES Katherine, "Lire et penser en milieux numériques : Attention, Récits, Technogenèse", Ed. UGA, 2016, accessed at.

[215] Royal Society for Public Health (2017). StatusofMind. rsph.org.uk. Retrieved April 13, 2021, from p. 3.

[216] JAMA P. BOERS E, AFZALI MH, Newton N, CONROD P. "Association of Screen Time and Depression in Adolescence. "2019, available at

[217] TWENGE, J.M., FARLEY, E. "Not all screen time is created equal: associations with mental health vary by activity and gender. Soc Psychiatry Psychiatr Epidemiol", 2021, available at

[218] ZWEIG Stefan, "Sigmund Freud, la guérison par l'esprit". Livre de Poche, 2010, 160p.

online harassment, etc.). In these digital and social ecosystems, the representation of happiness seems even more dependent on and biased by others than in real life. The omnipresence of screens and the need for social ties and recognition online overtax attention and degrade users' cognitive capacities. These negative effects gradually alter the benefits that web users derive from these digital spaces. Information comes and goes, and the algorithmic targeting of our preferences can lead to an overabundance of information, sometimes too negative or positive, to the point of impacting users' moods and desires. False information circulating on these networks, or the insatiable need to keep abreast of the latest news in real time, can lead vulnerable teenagers to be manipulated or even harassed, in areas as crucial to our society as their political or religious opinions, and sometimes leading to conspiracy talk. By losing control of our attention and our cognitive capacities, we are denied the right to be ourselves online, sometimes without understanding the urgency of the situation. Another major problem with these digital networks is their governance. While in law the problem is not so much the prohibition on data harvesting, which is in fact simply framed by the RGPD in many cases, governments can influence or even force certain social networks to make non-legitimate use of their platform, for example for geopolitical purposes (reference to the TikTok social network). Using a social network in a lawless state is risky for users, as it can be misused by a government as a tool for propaganda or mass surveillance, underlining the importance of pseudo-anonymity. In 2022, the Conseil d'Etat[219] published 17 recommendations in a study dedicated to the challenges and opportunities of social networks as applied to public authorities (institutions, local authorities, ministries). Some of these operational recommendations are particularly relevant, as they are based on the principle that decentralized digital identity (IND) would enable better control over the use a user wishes to make of the social networks they use.

2.2.1.2 Centralized, siloed digital identity

As a reminder and complement to the previous comments, the term digital identity 3.0 echoes an evolution towards a Web 3.0, also known as the "*Social Web*" or the "*Semantic Web*"[220] . The use of this term stems from the history of the Internet, which these sections aim to trace chronologically. To summarize, Web 1.0 enabled the simple reading of online data and information, Web 2.0 enabled the reading and writing of information, and finally, Web 3.0 enabled the reading, writing and ownership of online data (the latter being a combination of the original desire for decentralization

[219] Conseil d'Etat, "Réseaux sociaux: placer l'utilisateur au center", Event of September 27, 2022, available at the following address, p.17.
[220] Wikipedia contributors. "Semantic Web," accessed July 6, 2022, at

and community governance of Web 1.0 with the modern interaction functionalities of Web 3.0). Today and tomorrow, the Web will be an aggregate of 1.0, 2.0 and 3.0. At this stage, the terms "Internet 2.0" and "2.0 technologies", and "Web 3.0" and "3.0 technologies" respectively, refer not only to technologies, but also to the corresponding theoretical concepts addressed in this research. As digital identity is at the heart of our study, it is essential to distinguish its different types of computer functioning in order to understand the origin and future of online identity. First of all, the *siloed* digital identity model is currently the most widespread model for managing digital identities. It involves each digital service consumed serving as both identity provider and service provider. In other words, all the websites to which an Internet user logs on with a new username and password created when registering[221] , as with social networks[222] , as well as messaging platforms and any server, are part of this centralized, siloed identity model. While at the start of the Internet era, centralizing the data of a few Internet users appeared to be a simple and effective solution, as it expanded, this centralization of data gradually raised a number of issues, as some legal experts have pointed out[223] . Indeed, this centralized online identity offers little room for maneuver for Internet users: the systematic creation by the user of a new identifier attached to a password to access certain online services proves to be an often lengthy, insecure process, and today a source of friction for Internet users[224] . And yet, centralized identity remains the most widely used identification and authentication system for all types of online services. To remedy the problem of forgotten, stolen or lost user IDs, other identity models (also centralized) have been developed to limit user friction between each online service.

[221] *Dashlane* - ª company specializing in password management solutions - estimates that by 2022, the average American will have around 300 different web accounts and almost as many digital IDs, in *blog.dashlane.com/world- password-day*

[222] By way of illustration, this is the case for the Youtube platform, which provides a platform for video content (provider of an online service) while requiring its users to provide proof of majority to view certain content deemed sensitive (verifier/identity provider). On Facebook, too, ID may be required to post political content.

[223] "Any centralization of identifiers [digital identity] and, worse, of the means of exercising them raises the question of their misuse (potentially without leaving any trace) in the event of a breach of computer security", *op. cit.* "Digital identity 5.0 ", p.30.

[224] According to haveibeenpwned.com nearly 11,417,410,545 known accounts have been hacked according to several sources, accessed online on July 16, 2021. The causes of hacking are generally caused by a lack of attention on the part of Internet users, who (re)use passwords and/or identifiers that are too uncomplicated, but sometimes also due to service hosts (servers) whose cybersecurity management is deficient and leads to hacking.

2.2.1.3 Federated digital identity

While this second model of digital identity management is also centralized at the IT level[225] , like the previous one, an important difference remains in the fact that the identity provider and the service provider are two different legal entities that communicate with each other. Each time an Internet user wishes to access a digital service offered by a service provider, the latter calls on its identity provider to authenticate the user. In order to simplify accessibility, interoperability and navigation between online services for users, and also to reduce the risks of piracy, a federated digital identity model rapidly emerged between 2003 and 2005. This new method of combining digital identity connections enables the user to access multiple online services via a single login button (present on various online services, such as those indicating "Log in with your Gmail account" or "Log in with FranceConnect", as studied below). With this model, several identity providers establish agreements with each other and operate within a common technical trust framework. This communication between the identity provider and the service provider takes place via common IT and organizational standards and protocols, such as "OpenID"[226] , "SAML"[227] or "OAuth"[228] . It should be noted that these federation protocols can be used in a hybrid and complementary way[229] with decentralized digital identity standards. So, while decentralized identity standards may be decentralized in essence, they will probably be decentralized in conjunction with other conventional, centralized standards. This means that the IT solutions used by end-users will be both centralized and decentralized, i.e. hybrid (a term used throughout this research). Within the federated digital identity model, an organization can represent several entities, i.e. it can cumulate or possess several roles in terms of issuing a digital identity. This trust framework can be framed by competent public authorities, but can also be private, i.e. subject to multilateral contractual agreements between several entities (identity providers, service providers, government institutions, etc.). These standards and the concept of federated, third-party identity providers have become popular with the advent of certain identity providers and online network services such as Facebook or Gmail. In practice, these standards enable users, instead of logging on to a website with a username and password created for that site, to authenticate directly from their account.

[225] This means that data is stored on one or more servers under the control of one or more entities.
[226] OpenID is an open standard and decentralized authentication protocol promoted by the non-profit OpenID Foundation. Retrieved September 23, 2022, from
[227] Security Assertion Markup Language (SAML) is an open standard for the exchange of authentication and authorization data between parties (identity and online service providers).
[228] Open Authorization (OpAuth) is an open access delegation standard commonly used as a way for Internet users to grant websites or applications access to their information on other websites, but without giving them the passwords. Retrieved September 23, 2022, from
[229] Throughout this thesis, we consider that the term *hybrid digital identity* refers to a 2.0 and/or 3.0 digital identity systematically derived from a physical identity materialized by a civil and legal identity document.

Facebook or Gmail. However, this method relies on a cascading recovery of user data, which can jeopardize their privacy when there is a lack of transparency regarding this data management by online service providers (which is often the case). In this model, users' digital information is distributed between several identity providers, rather than being centralized in a single one. This organization of identity providers is generally referred to as a federation, because its players basically share a unique identifier for each user. In short, when a web user accesses a Facebook or Gmail account using their credentials, they are using a centralized, siloed digital identity model. When they access other services with credentials from these 2.0 platforms, it's a federated model. In both cases, user information and data are centralized by the identity provider(s). Ultimately, the federated approach to digital identities remains limited to those companies that participate in and adhere to such an alliance of connections between various, sometimes competing, digital identities and online services. What's more, this model does not systematically offer a concrete IT response to the need for transparency and traceability concerning the use of user data, which represents a major challenge to be resolved in order to generate digital trust.

2.2.1.4 User-centric digital identity

In response to the limits of systematic federation of these 2.0 digital identities by competing players (Google, Microsoft), a user-centric connection solution, also known as "ready-to-use identity", has emerged. This is a log-in service offered by a service provider to register and authenticate with other online services (also via a log-in button). This model is thus a mix between siloed and federated identity, combining their advantages through the principle of a single password for access to multiple services, while offering new technical sovereignty in terms of how it works. However, this model implies that a user stores directly on his or her personal device the credentials issued upstream by one or more identity providers, as mentioned above. In this way, unlike previous models, the user has control over his or her data on his or her own digital device. This can be any hardware or computing device, with or without keyboard and screen, that requires authentication, such as a PIN code. Given the current level of adoption and sophistication of cell phones, they are a particularly appropriate medium for this model of identity management, which in its more decentralized versions gives rise to a decentralized (IND) or self-sovereign (INAS) digital identity, both notions explored later (cryptographic issuance and storage of identity data directly on users' cell phones). In theory, this model is based on a

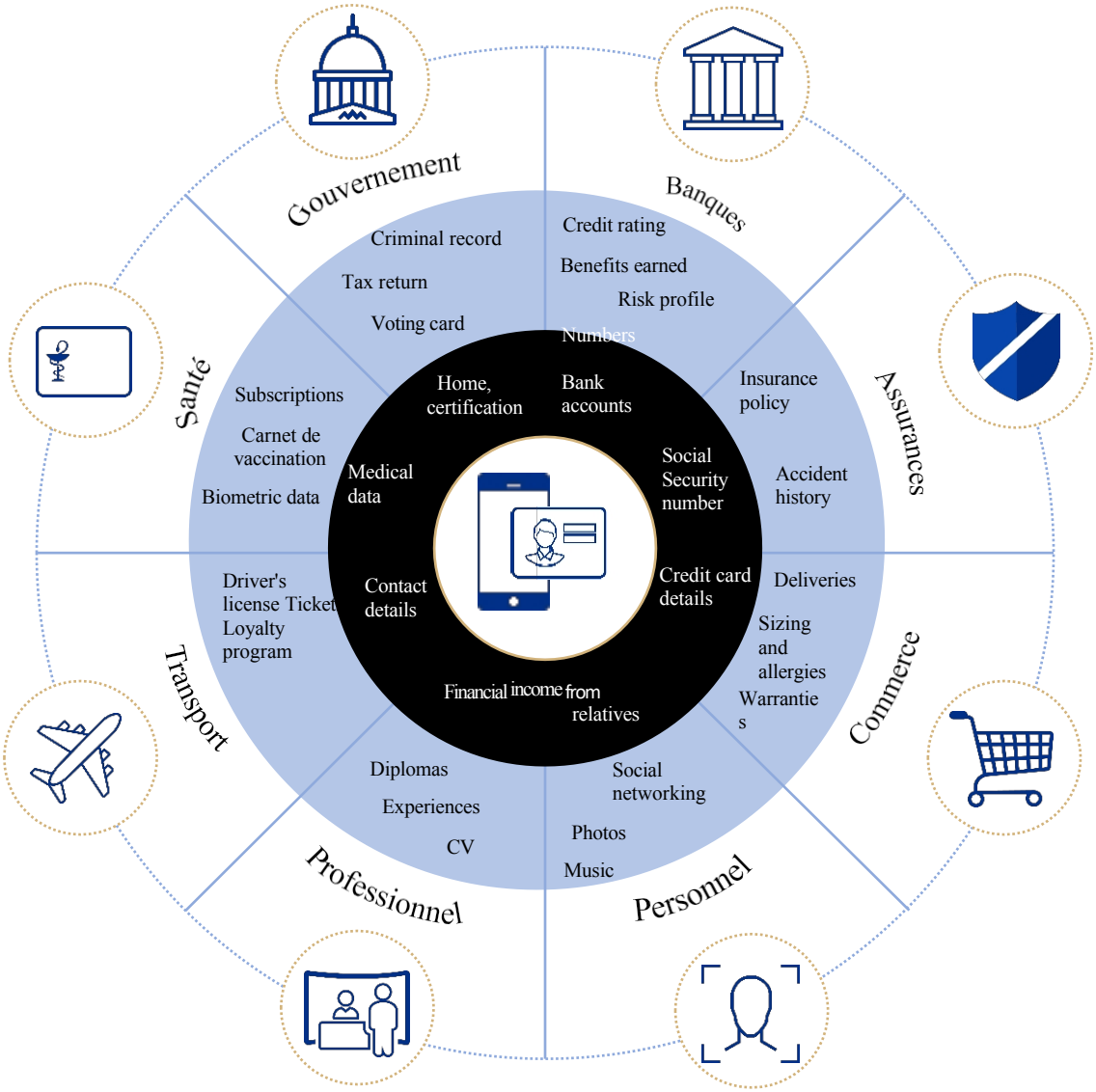
technical control of the user's identity data, a modality in line with the European Commission's desire for citizens to regain control of their digital identity[230] . In practice, this model can be seen as a more or less IT-decentralized one, in which the service provider can authenticate himself using a key stored in his IT device (instead of a username and password stored on the servers of an online third party). The fact that users have the ability to manage their data on their own devices, and the possibility of selecting which information to share with different service providers, leads us to consider this model as one of the technological and chronological evolutions of the decentralized digital identity model it inspires and incubates.

2.2.2 Markets, players and prospects for digital identity

The history of identity goes back as far as the existence of mankind and its need for identification. In other words, the need to identify individuals is intrinsic to human cultural and social activities. Digital technology has created certain asymmetries in the exercise of our offline and online rights, so profoundly has it transformed people's identity, as a recent study confirms: "*If we consider that the average person sleeps around 7 to 8 hours a day, the typical Internet user now spends more than 40% of his or her waking life online. The amount of time we spend online also continues to climb, with the daily average having increased by 4 minutes per day.*

[230] V. following parts.

(+1.0%) over the past year"[231] . For a holistic view of the size of the identity market, its various sectors and business cases[232] , we use this summary diagram:



Source : www.pwc.ch/en/insights/fs/digital-identity.html

In today's ubiquitous digital environment, the benefits of a recognized and interoperable digital identity are numerous, for citizens, public administrations and states, identity (attribute) providers and service providers alike. As a reminder, an identity provider can also supply services, and thus become a de facto service provider.

(i) Thanks to their digital identities, citizens can access cross-border online services simply, cost-effectively, reliably and securely.

[231] KEMP Simon, "Digital 2022: Global Overview Report", in *DataReportal,* January 26, 2022, available at
[232] Diagram taken from PriceWaterhouseCoopers (PWC), 2021, "Digital identity - Your key to unlock the digital transformation", accessed on September 26, 2022 at

(ii) With an interoperable digital identity, identity providers can access new sectors where there is a strong demand for identification (healthcare, transport) by offering their identification solutions (biometrics, centralized or decentralized digital identity). For public administrations, the implementation of a citizen digital identity can simplify certain redundant administrative procedures requiring a low degree of identity verification. In this respect, we are exploring the concept of *the* "*platform state*"[233] .

(iii) Online service providers can offer their services to users via simplified identification and authentication based on a trusted, legally-recognized state digital identity, such as the FranceConnect solution already mentioned. Its benefits include legal compliance by design, particularly with regard to the identification of individuals in the banking sector[234] , as well as a reduction in the costs associated with this identification.

The state's position as a trusted provider of digital identity is essential for private online service providers who use the state's digital solutions. The growth of the digital identity market depends on political or legal decisions that directly or indirectly impact the state and its institutions. As estimated by the McKinsey Global Institute, the economic stakes linked to digital identity are numerous. Countries that implement a digital identification policy could generate an average economic value equivalent to 3 to 6% of GDP by 2030[235] . Similarly, according to an information report by the French National Assembly dated July 8, 2020, the digital identity market is expected to represent more than one billion euros by 2029[236] . In 2021, this market will include numerous public and private players specializing in personal identity management[237] and, more generally, in the provision of digital trust services. While in the physical world, identity has historically been a public prerogative[238] , this is gradually fading in the face of new technological competition.[239]

---

[233] CHEVALLIER Jacques, "Vers l'État-plateforme?" in *Revue française d'administration publique*, 2018/3 (N°167), pp.627-637, available at

[234] Opening a bank account requires identification of the future account holder: the European anti-money laundering directives require banks to carry out an identification process known as *Know Your Custommer (KYC)*.

[235] Mc Kinsey Global Institute, "Infographic: What is good digital ID?", April 17, 2019, available at

[236] National Assembly Report N°3190, "Information report of July 8, 2020 on digital identity", accessed online on August 9, 2021, p.39.

[237] In particular, with the issuance of physical identities (national identity cards, passports) and/or digital identities (FranceConnect), and access to online services.

[238] Notably through the issuance of official identity documents such as the new electronic national identity card (CNIe) supplied by IN Groupe to the Agence Nationale des Titres Sécurisés (ANTS).

[239] Thanks to the massive harvesting of their users' personal data, some private players offer a derivation of people's digital identity, in exchange for simplified access to third-party partner services (online shops, social networks, etc.).

private digital identity solutions[240] (Apple Wallet, Google sign-in)[241] federated, and deployed by certain digital giants (GAFAM and BHATX mentioned above). The aim of these new private digital identity solutions is to offer all-inclusive platforms for service providers (from digital customer onboarding to authentication and targeted advertising). During the COVID- 19 crisis, there was a significant increase in fund-raising for companies developing technologies enabling the online identification of digital identity users.

What all current and aforementioned digital identity management systems have in common is that they are centralized to a greater or lesser extent by trusted third parties. Today, this notion of digital trust - and the adjacent one of sovereignty - can be reinforced thanks to the emergence of a new method of decentralized digital identity management using blockchain technology, and to determine which of the blockchains already on the market is best suited to the needs of the players involved. In reality, these interactions today rely on trusted third parties (public or private). Are Internet users really willing to take back control of their digital identities? According to a recent study by Accenture, it seems that people naturally trust public institutions whose public interest is their essence: "(...) *(84%) of those surveyed said they would be willing to share their personal information with a government service in exchange for more personalized customer service*"[242] . However, the use of decentralized digital identity systems developed by private companies, which are examined below, will have to prove their worth if they are to acquire a level of trust similar to that accorded to public institutions. Before introducing the state of the European 3.0 digital identity market, a preliminary comparison becomes relevant in order to introduce the contributions of this decentralized digital identity compared to the current use of centralized (2.0) digital identities:

[240] As a reminder, an important distinction remains: *identification* is not the responsibility of the individual, and involves a third-party service registering and managing his or her digital identity; *authentication* is the responsibility of the user, who registers or identifies himself in order to access a third-party service. However, some digital identity providers may jointly provide identification and authentication services to Internet users. V. Glossary.
[241] Apple announced in September 2021 to provide some US states with citizens' driver's licenses and civil IDs directly from its Digital Wallet 2.0 (Apple Wallet). The project is progressing slowly, as new technologies and processes are added to meet the different needs of these states. The deadline for implementing these "Real IDs" is expected to be 2025. "Apple announces first states signed up to adopt driver's licenses and state IDs in Apple Wallet", in *apple.com*, available at
[242] ACCENTURE, "Citizens Willing to Share Personal Data with Government in Exchange for Enhanced Customer Services Accenture," February 24, 2020, accessed online June 10, 2022 at.

IT and legal considerations	**Centralized digital identity (2.0)**	**Decentralized digital identity (3.0)**
Digital identity(ies)	• Controlled by one or more entities, often with little IT transparency. • Fragmentation across multiple platforms and online services. • Technically transmissible to a third party without obtaining consent or informing the interested party (low transparency and total dependence for users).	• Partially or fully transparent and user-controlled. • Portability across multiple platforms and online services. • Technically non-transferable to a third party without cryptographic consent consent.
Data management and security	• Complex use of multiple passwords and IDs. • The centralized servers of these online services are favorite targets ("honeypots") for hackers. • Limited verifiability of information and data (technically time-consuming for online services).	• Public, private or hybrid blockchain infrastructures (public and private key: "PKI")[243] . • End-to-end data encryption by design (programmed confidentiality). • Limited exposure of data to attacks thanks to data revocation and compartmentalization (see "eIDAS-2").
Personal data management	• Partial and/or end-to-end encryption possible, although not systematic. • Data traceable only by centralized third parties with varying levels of cybersecurity. • Revocation and cryptographic suppression of data are computer-impossible (due to their duplication and dispersion on the Internet). • Data control by third parties more or less trust (technical dependency).	• Attributes assumed to be portable across all online services (verifiable data evidence on an open or closed blockchain). • Centered on the user, who controls all or part of his or her data through a decentralized decentralized digital identity (v. "PIND"). • Data can be deleted at any time, even after transmission to an online service.

[243] "A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, distribute, use, store and revoke digital certificates and manage public key encryption," in *Wikipedia*, accessed online April 22, 2021.

		• Partial and selective disclosure of data possible.

2.2.2.1 Digital identity in Europe

Since 2014, the European Union has attempted to harmonize digital services requiring a digital identity, thanks to the adoption of the eIDAS Regulation already mentioned and studied in the second title of this study. While this legal strategy has had its benefits, it has also limited innovation and the mass adoption of digital identity solutions by the private sector. As a result, only large technology companies have been able to design solutions that comply with the eIDAS Regulation and the RGPD, also studied below. European Union member states were forced, with the European Parliament and Council Regulation of June 20, 2019[244] , to publish new-generation national identity cards (CNIe), before August 2, 2021, on pain of financial penalties. While some countries had already implemented the new rules and technical standards, such as size, physical security and digital capacity with an electronic chip, imposed by the Regulation for new-generation national identity cards, other countries, including France, were lagging behind due to political and institutional differences. In practice, the aim of applying the Regulation from 2021 is to harmonize national e-ID cards with a minimum level of interoperability, while ensuring their integrity and promoting their use for a wide range of online and offline purposes. In 2022, Germany (IDUnion) and Spain (Alastria) signed a Memorandum of Understanding to collaborate and exchange technical, regulatory and operational knowledge on digital identity. Two similar bilateral declarations were signed between Germany and Finland, and between Germany and the Netherlands. Also worthy of note is the Europe-wide initiative known as "Gaia-X", which proposes several digital trust infrastructures in compliance with EU law[245] . These joint initiatives testify to mutual commitments to develop decentralized industrial identity solutions that complement the digital identity 2.0 solutions deployed within the EU.

[244] Regulation (EU) 2019/1157 of the Parliament and of the Council of June 20, 2019 on increasing the security of identity cards and residence documents of EU citizens and their family members exercising their right to free movement, EUR-Lex, accessed March 23, 2022 at.

[245] The Gaia-X compliance and labeling framework defines three levels of compliance: (i) *Gaia-X Level 1* is the basic level, guaranteeing that the service adheres to the founding and technical principles of Gaia-X; (ii) *Gaia-X Level 2* goes beyond this to reflect a higher level of transparency and security, as Level 2-labeled services must also offer an option enabling companies to ensure that processing and data are carried out on European soil; and (iii) *Gaia-X Level 3* goes even further, advocating European sovereignty. *Level 3* guarantees not only European location and operationalization of services, but also immunity to the extraterritoriality of certain non-European laws.

As of 2021-2022, as illustrated in the following diagram, France does not yet have a structure to federate players in the decentralized digital identity sector. Nevertheless, several initiatives are underway, such as the Alliance Blockchain France (ABF) detailed below, or the consortium of companies named Archipels[246] . The aim of these initiatives is to create shared, multi-sector, user-centric 3.0 infrastructures and networks.

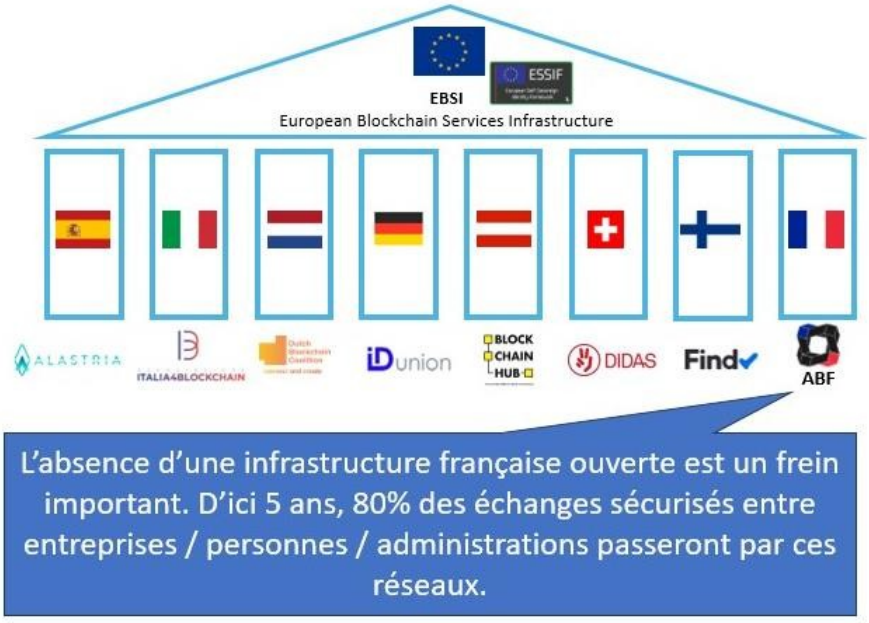


Diagram based on a presentation by the ABF to the DGE on March 29, 2022.

The following sections offer a comparative legal-technical analysis, which is of course not exhaustive, but which focuses on the current and future challenges of certain pioneering member states (Germany, Spain and Estonia) in terms of digital identity in Europe.

2.2.2.1.a Regalian digital identity in France: FranceConnect and CNIe

Currently in France, two major digital identification systems are available to citizens: FranceConnect and the electronic digital identity card (CNIe), which have several technological components, as we shall see. First of all, FranceConnect is a government-run authentication service designed to simplify online procedures for French citizens. Technically, this federated "*Single Sign On (SSO)*" identity system[247] works using a certain amount of aggregated minimum identity information (pivot data), and enables citizens to connect to numerous public and private online services, as well as to Internet service providers.

[246] Archipels, "La plateforme WEB 3, pour des données et des identités vérifiables", available at
[247] Based on the *OpenID Connect* protocol.

accredited services such as the health insurance fund or the tax office. FranceConnect is an "*information system enabling users to carry out administrative procedures or formalities electronically*"[248] . This identity association system was born in response to GAFAM/BHATX's digital identification and authentication systems. A major difference distinguishes this regalian federated identity model from the aforementioned identity federations of major digital companies. In the former case, it has no commercial purpose[249] , whereas in the latter it does. FranceConnect does not store any of its users' personal data, as they only pass in transit between the players in this federated digital identity model, of which only a pseudo-anonymous trace is kept (FranceConnect places itself upstream or downstream of an identity attribute provider and then masks the latter's origin). With this system, initiated in 2015[250] , and completed since March 31, 2023 with the new digital identity designated YRIS[251] , the French government's aim is to remain a key player in the digital sphere, representing a source of digital trust. From the user's point of view, FranceConnect is a simple login button integrated into online services that are currently provided by the State. Each user is assigned a unique identifier to access the service. During this interaction, primary personal data is temporarily collected by an authorized identity provider. This data is then transformed into a pseudo-anonymous identifier, which is used to verify a match with the original identical data, which has been registered and stored by the State in the National Individual Identification Register (RNIPP). Once this technical match has been assured and certified, the unique identifier is used by FranceConnect as proof of a person's root identity, which can then be identified or authenticated by a third-party identity provider. FranceConnect thus represents an easy-to-access tool, while enabling users to register once for multiple subsequent authentications. In 2022, a new service called **FranceConnect+** was launched. This service offers a higher level of trust, differentiating it from the initial FranceConnect service. This version is currently free of charge and is being tested until 2024 in various sectors, including healthcare, social services, education, transport[252] and property and vehicle rental. The Assistance publique des Hôpitaux de Paris (AP-HP) is currently testing the **FranceConnect+** solution to achieve a high level of trust within the meaning of the eIDAS regulation studied below, thanks to the identity of its users.

---

[248] Ordinance no. 2005-1516 of December 8, 2005 on electronic exchanges between users and administrative authorities and between administrative authorities, consulted online on March 23, 2022.

[249] Order of May 11, 2020 on t h e experiment to extend the scope of teleservice partners.
"FranceConnect", JORF n°0124 of May 21, 2020, *v.* art.3: "they [private services connected to FranceConnect] may not market personal data obtained under this order even with the user's consent and may not transmit them outside the European Union".

250Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé "FranceConnect", Légifrance consulted online March 23, 2022.

[251] This is the new digital identity that will replace the Mobile Connect & Moi (MCEM) identity from 01/04/2023, enabling access to numerous government services via FranceConnect.

[252] The use case of transportation is relevant to decentralized digital identity, as each person has a right to his or her journey as soon as he or she possesses a means of proof attesting to the purchase of this right (plane tickets, train tickets, etc.).

provided by Groupe La Poste. In domestic law, digital identity has not been defined by the legislator, and its presence in positive law seems deliberately restricted. Article L.226-4-1 of the French Penal Code refers to the offence of identity theft without explicitly defining the notion of digital identity, preferring to use the following wording "*when committed on an online public communication network*"[253] . Nevertheless, this circumvention, designed to avoid taking a position on what (digital) identity is, is based on a principle of neutrality that is generally accepted in law.

Discussions about a national digital identity have been going on in France for over 20 years. It therefore seems appropriate to give a brief French overview of the many digital identity projects carried out by the former Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État (DINSIC), now the Direction Interministérielle du Numérique (DINUM) supported by the Ministry of the Interior. For over a decade, several other electronic resources have been developed, such as the Data.Gouv platform (2011) or the Alicem mobile application (2019), now replaced by the SGIN application[254] . With these projects, the French government is asserting its ambitions with regard to digital identity, with the aim of providing simple and secure digital identification, guaranteed by the State. To date, the digital component of the long-awaited CNIe has been enshrined in Decree no. 2022-676 of April 26, 2022, authorizing the aforementioned SGIN service as a means of electronic identification[255] . This mobile application enables individuals to prove their identity online to public and private services, and to control the distribution of their identity data, thus constituting a first step towards a digital identity controlled by users. The application is currently optional, and by the end of 2023, several full-scale experiments will have been carried out to send "*single-use, authentic and secure credentials* [probably verifiable certificates]"[256] . However, certain limitations currently exist for these national initiatives through a lack of understanding of online service providers and identity providers, a lack of transparency and supervision of private subcontractors for data storage and transmission, a lack of staff training, and certain ambiguities in public-private relations followed by insufficient political responsiveness. Although the creation of a French digital identity is a sovereign responsibility of the State, it will take a strong normative, institutional and political influence to achieve a supranational digital identity, in addition to the national digital identity. France is currently behind other member states in notifying its digital identification scheme.

---

[253] Art. 226-4-1 of the French Penal Code, in *Légifrance*, consulted online on September 15, 2021.
[254] "France Identité, gardez la maîtrise de vos données d'identité" in République Française, available at
[255] Decree no. 2022-676 of April 26, 2022 authorizing the creation of an electronic means of identification called "Service de garantie de l'identité numérique" (SGIN) and repealing decree no. 2019-452 of May 13, 2019 authorizing the creation of an electronic means of identification called "Authentification en ligne certifiée sur mobile", available at the following address
[256] NEGRONI Angélique, " Les cartes d'identité vont bientôt être dématérialisées sur smartphone ", in *Le Figaro*, July 12, 2022, " Pour l'heure [2022], 1000 personnes qui se sont portées candidats testent ce service. By next September [2023], the number will have risen to 4,000", available at the following address

who have already notified their respective schemes, some since 2018 (Estonia, Spain, Belgium, Luxembourg)[257] . Without notification to the European Commission, FranceConnect will not reach the Holy Grail of mutual recognition so promised by the eIDAS Regulation. This delay in France is due to discrepancies in technical standardization and political decisions, but it does allow France to position itself as an observer of the digital identity solutions already deployed by its European neighbors. When FranceConnect is notified, it could be difficult for the solution to establish itself as a model, either because it is behind the times, or because its business model is largely based on public, rather than private, digital identity solutions. The new electronic digital identity card (CNIe) is based on a new French technical standard called PACE+PIN[258] . It promises a new method of digital authentication for French citizens[259] , thanks to a contactless authentication capability protected by a four-digit code known only to its holder[260] . Thanks to a new parliamentary proposal that amended the French Identity Protection Act no. 2012-410 of March 27, 2021, the CNIe is likely to be coupled with decentralized identity mechanisms as well as the FranceConnect system, so as to offer identification as well as authentication of substantial or high levels under the forthcoming adoption of the proposed amendment to the eIDAS Regulation ("eIDAS-2"), studied in the first part of this research.

However, although **FranceConnect+** represents a first step in the establishment of digital trust in terms of sovereign digital identity, it is clear that the system still faces a number of IT challenges. Indeed, while the growth in the number of users of this system is benefiting[261] , FranceConnect currently offers a limited number of public and, above all, private services (1,300 online services by 2022) compared with citizens' huge, ongoing digital identification and authentication needs. This effective, but limited, growth in the number of online services means that the service offered by FranceConnect will be difficult to deploy. In addition, FranceConnect's IT security was put to the test in 2022[262] . In addition, the centralized nature of FranceConnect, which depends on federated interactions with accredited identity and service providers, represents an identity 2.0 scheme that predates identity 3.0, with a view to moderate decentralization in the short to medium term. To avoid any

[257] A real-time overview of Member States' pre-notified and notified e-ID schemes is available at the following address. The French digital identity scheme (FranceConnect) was finally notified in February 2021.
[258] This new standard is derived from the international standard "Identification-Authentification-Signature European-Citizen-Card (IAS-ECC)", *v.* Wikimedia, available at the following address
[259] "The identity card will contain two chips, one reserved for verification of the bearer's identity by means of fingerprints (the so-called 'regalienne' chip), which could only be read by the authorities authorized to carry out an identity check, and the other reserved for the functionality introduced by the present article ('daily life' chip), which could be read by commercially available devices connected to a personal computer", *op. cit.* Senate. 1er June 2022. Proposition de loi relative à la protection de l'identité, available at the following address
[260] By analogy, this system works like that of cell phones, which have a "PUC" master code and a "PIN" derived authentication code.
[261] FranceConnect will have 30 million users by 2022.
[262] DOMENECH Claire, "Des milliers d'euros volés via le site des impôts à cause du bouton FranceConnect", 2022, in *Capital.fr*

The future version of FranceConnect and the SGIN application, and their interface with the CNIe, will be based on a combination of mass education and IT compromises, in particular political confrontation between these two digital identity management systems. Ultimately, the above findings and challenges suggest that the decentralized identity solutions under development (including those backed by blockchain) in France will be compatible with the "pivotal" digital identity of **FranceConnect+**, but also with the CNIe[263] . To achieve this, FranceConnect must work with DINUM[264] and ANSSI[265] to understand how to handle this future technical cohabitation, particularly in view of the forthcoming adoption of a European digital identity wallet, discussed below. For this, a specifically dedicated legal framework relating to the non-commercialization of collected data must persist, so that the State does not unwillingly become a supplier of identity data for commercial purposes (as is tending to be the case in Spain). However, in 2023, FranceConnect was legally designed to connect to a trusted website managed by the State and its institutions. In this respect, the decree of November 8, 2018 giving birth to and framing FranceConnect could be amended accordingly to enable this system to potentially manage decentralized identity attributes (VC, DID)[266] which are studied below. Moreover, in a thematic dossier published in March 2023, the CNIL discusses and encourages the use of decentralized digital identities. Finally, it should be noted that, unlike Estonia, France has chosen not to impose a single regalian digital identity, i.e. to leave users free to entrust their personal data to an operator of their choice.

2.2.2.1.b Launch of Alliance Blockchain France

For several years now, the European Commission has given priority to funding essential technologies, particularly in the fields of cybersecurity and artificial intelligence[267] and trusted cloud hosting[268] . This desire is accentuated by an environment where digital trust is increasingly critical, and within which blockchain technology can be a new catalyst of trust for securing digital interactions. Now

[263] At present, the electronic component of the CNIe is deactivated for legal reasons, i.e. because it is legally impossible for private companies and services to use the electronic part of the CNIe. This means that every French citizen receives his or her CNIe, and for the time being can only use it as a travel document within the EU, or as proof of identity in France. The digital capability of this card is therefore deactivated for the time being, blocked by default as it leaves production, until amendments are made to allow private companies and citizens to interact with this digital functionality of the CNIe.
[264] Interministerial digital department (DINUM)
[265] The French national agency for information systems security (ANSSI).
[266] See *infra*, II, Title 1, 1.3.1.
[267] Proposal for Regulation 2021/0106 of the European Parliament and of the Council of 24 April 2021 laying down harmonized rules on artificial intelligence (artificial intelligence legislation) and amending certain Union legislative acts.
[268] CE, "Cloud computing. Shaping Europe's digital future". Retrieved September 27, 2022, from

Perceived as a new technological challenge on a community scale, blockchain has come to the fore in the wake of the health crisis and the growing need to secure online exchanges. The Alliance Blockchain France (ABF) was born out of a desire to offer decentralized digital identities (in reality hybrids in IT terms) to facilitate data sharing, drastically reduce fraud and online disputes, while automating contract execution (smart contracts). It is a not-for-profit initiative that aims to provide a new sovereign and partially decentralized digital infrastructure on a national scale thanks to blockchain technologies, starting with the digital identity sector. With its 17 founding members[269] , this association governed by the law of July 1er 1901 federates French public, academic and private players to promote the emergence and development of a cutting-edge national ecosystem around distributed electronic registries (blockchains), with the aim of developing innovative digital services, without providing digital identity attributes, but simply an ecosystem of recognized and trusted players. The association also aims to develop initiatives that have a positive impact on democratic values and the environment. More specifically, it aims to create first-level infrastructures managed on a shared basis by its members. In practice, the creation of a consortium between major economic players is a long and complex process, involving the implementation of centralized or semi-decentralized governance, often difficult to balance for companies with different resources and strategies. Until now, the main way of guaranteeing the legal conformity of such a grouping of players has involved the use of a hybrid blockchain, i.e. the creation of an IT and contractual consortium between several players.

2.2.2.1.c Estonian digital identity

Estonia is regularly cited as a European pioneer in the field of regalian digital identity. For 20 years now, every Estonian citizen (around 98%)[270] has had a digital identity card (now similar to the French CNIe), enabling access to several thousand public and private services[271] , including dematerialized services via cell phone. As well as being a step ahead in terms of time, Estonia is an example to follow when it comes to the technical dimension of its digital identity. In fact, a private state blockchain ("*KSI blockchain*") provides each public institution with a high level of security and IT interoperability between their systems and services, thanks to

[269] V. official website of Alliance Blockchain France (ABF) at www.alliance-blockchain.org
[270] Minutes of the round table on "The digital transformation of schools in Estonia and France", co-organized by France Stratégie and the Estonian Embassy in France, May 5, 2017.
[271] Access to public transport infrastructures, online voting, going to court, retrieving medical prescriptions, signing contracts, creating and managing a company, registering the name of a newborn child, etc.

to a distributed platform ("X-Road")[272] . In addition, this system, which is actually more *distributed* than completely *decentralized*[273] , guarantees citizens technical and legal confidentiality of their data. While this system has proved effective in managing a large number of transactions, a certain technical opacity remains as to how this IT architecture actually works. While this lack of transparency may be justified by a desire not to reveal any technical flaws to the world's developers, it is likely that opening up the infrastructure's source codes would benefit it in the long term. To illustrate the above, a security flaw was detected in 2017 on the Estonian CNIe, impacting over 760,000 citizens[274] (impossibility of access to certain online services and impersonation of certain Estonian citizens). There is no doubt that the 3.0 IT architecture currently used in Estonia will one day be compatible with decentralized identity standards, to provide an additional IT layer of trust for Estonian citizens. It should be noted that an IT compromise (hybrid versus decentralized solutions) will probably be necessary to prevent citizens from taking full control of the issuance of their identities, i.e. to allow them only to manage and not to issue their identity data, as will be explored later.

2.2.2.1.d Digital identity in Spain: DNIe and Alastria

Decree no. 1553 of December 23, 2005, issued in application of Law no. 59/2003 of December 19, 2003, introduces a computer chip into the electronic version of the identity card ("*documento nacional de identidad electronica - DNIe*"). This chip contains all the personal data available on the printed version of the card, the document holder's photograph, digitized signature and fingerprint template, as well as authentication certificates (which enable the holder to be identified) and signature certificates (which enable online documents to be signed electronically)[275] . The DNIe can be read by a card reader or by an NFC-enabled cell phone[276] , via a mobile application called "Mobbeel"[277] . The latter enables citizens to identify themselves only once to access a multitude of public and private services (federated identity model similar to FranceConnect): automotive, online gaming, travel and tourism, etc. After reading the DNIe, it is clear that

[272] For more information on the IT specifics of this private blockchain and platform, available online at
[273] In computer science, a distinction between the notions of "distribution" versus "decentralization" is commonplace. We propose to revisit this distinction in a dedicated section.
[274] "Security flaw forces Estonia ID 'lockdown'", in *BBC News*, November 3, 2017, accessed online March 23, 2022.
[275] Spanish Ministry of the Interior (ministerio del interior), Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, 2005, accessed online on March 23, 2022.
[276] Wikipedia contributors, "Near-field communication (NFC)", 2022, accessed online March 23, 2022.
[277] "Mobbeel", accessed online on March 23, 2022.

citizens are likely to be asked to enter their PIN code to access the public or private service concerned (this PIN code is similar to the French PIN, which has not yet activated this functionality). What's more, this PIN code must be updated every 30 months by the citizen, who must then physically visit the DNIe-issuing offices to do so. Law 6/2020 of November 11, 2020[278] regulating certain aspects of electronic trust services provides further details on access to online services via the Spanish electronic identity card. These services include some from the private sector. These may include banks (Kutxabank, Unicaja Banco, Barclays), telecoms services (Vodafone), insurance companies (MAPFRE) and others. DNIe 2.0's digital capability offers Spanish citizens the possibility of accessing certified online services enabling electronic signatures, administrative procedures, doctor's appointments and other activities of daily life. Under Spanish law, there is nothing to prevent private companies from accessing citizens' personal data available on the DNIe chip (no restricted access as in France). This is illustrated, for example, by Kutxabank, which makes no secret of the fact that it collects biometric data for commercial purposes (fingerprints and facial recognition) from citizens/customers[279] . The Spanish data protection authority does not comment on this issue. In legal terms, the Mobbeel application - like the German application - provides a high level of authentication within the meaning of the eIDAS Regulation, in that it enables citizens to embark (initial identification) through their biometric data[280] . When it comes to decentralized digital identity, Spain is one of the most advanced EU countries. Indeed, a consortium of private players ("Alastria")[281] was born in 2019 on the subject. The Alastria consortium is attracting growing interest and now includes around a hundred players and an expanding blockchain infrastructure. Its structure (IT, legal and in terms of governance) makes it one of the most respected in Europe. However, unlike the German "IDunion" consortium, which was initiated by German public and private players, Alastria lacks support from Spanish public institutions. This last element is crucial if Spanish institutions are not to be the vectors, as in France, of such political brakes on the use of 3.0 technologies in the supposed service of citizens' rights.

[278] WIPO Lex, 2020, available online at
[279] Kutxabank, "*Particulares*", available at the following address
[280] Available at the following address
[281] Available at the following address

2.2.2.1.e Digital identity in Germany: the IDunion consortium

In 2021, the German government unveiled a new digital identity application "*AusweisApp2*"[282] coupled with the German national identity card. Authorities can now issue this new electronic identity card to all German citizens and foreigners aged 16 and over[283] . According to the eIDAS Regulation, this mobile application coupled with the German national identity card ensures a high level of trust[284] (in the same way as Spain, whose electronic identification scheme also has a high level of guarantee)[285] . Governikus[286] , based in Germany, was commissioned to implement the German reference digital identity. It implemented the related technical infrastructure, including the AusweisApp2 application, available on Windows, MacOS, Android and iOS. It thus represents the standard application for all government-related online services in Germany. Its operation is transparent, and it is supplied under an open source license (EUPL 1.2)[287] (unlike applications from other countries). While this new German CNIe is comparable to the one currently deployed in Spain and France, and more generally in the EU (due to the common rules emanating from the eIDAS Regulation), a consortium of private players called (IDunion)[288] is currently developing use cases linked to the blockchain[289] and decentralized identity, and will most likely use the current digital identity capabilities of this CNIe. As a result, the German digital identity model is well positioned to provide a distributed (IND) or self-sovereign (INAS) digital identity. The French model could draw inspiration from the latter, both technically and politically respectively, for example by taking inspiration from the political manifesto signed in 2021 by Germany with Finland for cooperation on decentralized digital identity[290] .

[282] Available at www.ausweisapp.bund.de
[283] *Op. cit*. *at* the following address
[284] Available at
[285] Electronic identification schemes notified in accordance with Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, 2019, page 1-3, available at.
[286] Available at
[287] Commission Implementing Decision (EU) 2017/863 of May 18, 2017 updating the EUPL open source software license to facilitate the sharing and reuse of software developed by public administrations. Available at the following address
[288] Available at
[289] This consortium has set up a *hybrid blockchain* whose data can be accessed in real time at the following address
[290] "Nederland gaat met Duitsland werken aan digitale identiteit, ministerie van Binnenlandse Zaken en Koninkrijksrelaties", September 23, 2021, available at.

2.2.2.2 A European blockchain (EBSI) for a distributed identity

In 2017, some researchers were already estimating[291] that governments could create their own regulated blockchains (hybrid or private blockchains) in an attempt to transcribe certain social governance rules into code: "*while governments might not succeed in regulating blockchain technology comprehensively, they could nevertheless rely on blockchains as a means of enforcing their own laws and regulations more effectively and automatically.*"[292] . And so, just a few years after these words seemed to be confirmed, on April 10, 2018, twenty-one member states plus Norway agreed to sign a declaration creating the European Blockchain Partnership (EBP) and leading to the creation of a common European blockchain infrastructure: the "*European Blockchain Service Infrastructure - EBSI*"[293] . Since 2020, EBSI has been deploying a consortium network of (36)[294] blockchain nodes across Europe[295] , supporting applications focused on specific use cases[296] . EBSI is the first blockchain infrastructure to be piloted on an EU-wide scale, and for the time being only for the public sector. EBSI is conceived as a market-friendly ecosystem, based in theory on open IT and legal standards and a transparent governance model. EBSI has emerged to provide a common response to recurring problems encountered by projects using blockchain technology. It is a so-called "*multi-chain"* infrastructure, meaning that it is interoperable and compatible with different protocols and other blockchain infrastructures of varying degrees of openness (public, private or hybrid blockchains, as discussed below). In theory, EBSI is built around four founding principles, which we feel it is important to summarize and analyze in table form

:

[291] De FILIPPI Primavera, "Blockchain and the Law," in *Harvard University Press*. *op. cit.*
[292] *Ibid*. Location 3762 on 7004.
[293] ELIE Pauline, SEGHIER Neil, LANGLOIS-BERTHELOT Thibault, "Blockchain and Digital ID Wallet: towards a decentralized European identity?", May 2022, Workshop No. 2, Les Temps Numériques, scientific paper available at.
[294] V. Appendix 6, Focus 3.
[295] Note that only 11 of the 36 nodes are validator nodes. EBSI. (2018). European Commission. Retrieved April 1, 2022, from
[296] For the time being, it operates via "*Pre Commercial Procurments" (PCP)* for various pilot use cases, enabling different players to be selected (initially exclusively from the public sector, then progressively from the private sector).

(i) Becoming a digital commons	(ii) Providing trusted governance and harmonization of digital interactions	(iii) Accessibility and IT transparency	(iv) Compliance with regulations and to European values
EBSI administration must serve the common good, and it is incumbent upon it to limit its use to public services in the first instance, and to open up to private players in the second. Bringing these players together will ensure this desire to position EBSI as a public good at the service of citizens, businesses and member states as a whole. In 2022, EBSI therefore represents a hybrid blockchain infrastructure that should not be confused with public blockchains. This research assumes that the Bitcoin blockchain[297] is considered a universal digital commons, and one that is politically and socially neutral. In contrast, EBSI is considered an artificial digital commons, which is created by a small number of public and private actors and is regulated politically, legally and economically. Consequently, it is assumed that the crypto-asset associated with the blockchain Bitcoin is a token	In principle, EBSI's governance system ensures that decisions are taken by consensus between its internal stakeholders (member states). This political centralization ensures that decisions are tailor-made and consensual. of decisions, in particular to ensure the legal and economic adequacy of services and infrastructures deployed within the EU. It is important that EBSI's governance promotes and maintains harmonized technical and IT requirements to avoid the multiplication of the different blockchain protocols supported, while avoiding the emergence of incompatible systems. supported blockchain protocols, while avoiding the emergence of incompatible 3.0 systems.	As far as possible, the source code of EBSI's infrastructures and services should be accessible to a large number of developers, to enable maximum auditing and IT security. and security. What's more, this transparency promotes healthy competition between identity providers, service providers and the private sector in general. It is nevertheless from recognize current dependence from EBSI towards public blockchains that are the	EBSI must comply with the current interpretation and future updates of the RGPD as well as with eIDAS and other regulations (in particular when financial tokenization occurs, i.e. when when associated will be associated with a crypto-asset - stable or not - for IT and/or commercial purposes)[298] . EBSI must comply with all relevant regulations to ensure the protection of data and guarantee the security of transactions carried out on platform.

		main	

[297] V. Appendix 3, Focus 6.

[298] The introduction of one or more crypto-assets (utility or payment tokens) within one or more of EBSI's blockchain infrastructures has been politically rejected to date (2022). Indeed, as this is a *hybrid consortium blockchain*, there is still a distrust, even a form of mistrust, towards *public blockchains* (due to their native crypto-assets), in European political and institutional spheres.

pure' and incensurable, while future EBSI digital tokens would be considered 'artificial'. EBSI's blockchain is expected to host artificial digital tokens within the next few years, probably eventually including a euro. cryptographic.	This harmonization must also ensure that only protocols that comply with Community law are integrated, in order to avoid any legal conflicts.	sources innovation.	

In 2023, EBSI is focusing on three main categories of use: decentralized digital identity, digital traceability and trusted data sharing. For decentralized digital identity, EBSI aims to establish a more autonomous identity model in Europe that allows users to control their identity across national borders. For digital traceability, EBSI aims to create reliable digital audit trails, i.e. to automate compliance checks and proofs of data integrity. In terms of data sharing, EBSI aims to facilitate communication between EU customs and tax authorities, particularly with regard to identification numbers and the single import window (VAT & IOSS)[299] . EBSI's operation is currently limited by successive use-case funding[300] , which will continue until 2023 or 2024. From 2024 onwards, and by 2026[301] , the blockchain could be fully opened up and scaled up. Technical recognition of public blockchains seems important to support politically for the future of EBSI, in particular to foster sustainable innovation of this whole 3.0 ecosystem (via political and possibly legal recognition with adapted legal rules). It is also important to note that EBSI faces a number of challenges in the short term, of an IT, legal[302] and political nature. Setting up a system of governance involving a large number of players requires time to negotiate and implement solutions that are still in the experimental phase. On February 14, 2023[303] , the Commission

[299] "In order to better adapt VAT collection to the reality of cross-border e-commerce, and to secure its collection in the country where the goods are consumed, a new optional taxation system has been created: the IOSS (Import One-Stop-Shop) system. The scheme consists of a one-stop VAT shop, which simplifies the reporting and payment of VAT on distance sales of imported goods worth 150 euros or less". Regulations on the one-stop VAT shop or IOSS. 2022. V. the portal of the French Customs and Excise Department at the following address

[300] *Op. cit.* This financing of specific use cases is called "Pre-Commercial Procurement (PCP)", which operates in successive phases (Phase 1, Phase 2A - current in 2022 - Phase 2B), "European Blockchain Pre-Commercial Procurement", October 2021, in *Shaping Europe's Digital Future*, available at

[301] DUSSUTOUR Olivier, Managing Director, Nexus: "Thanks to the European work in progress, we may have the chance to present the first massive decentralized identity schemes by 2026", Interview at the International Cybersecurity Forum (FIC) on 09/09/2021, round table: "What alternative models for identity?

[302] By way of illustration, there were differing opinions as to whether decentralized identifiers (DIDs) should be anchored directly on the EBSI blockchain, or whether proofs of these DIDs should simply be used.

[303] "The aim of the 'European Blockchain Regulatory Sandbox' is to facilitate cross-border dialogue with and between regulators and supervisors on the one hand, and companies or public authorities on the other.

The European Commission has launched a "legal sandbox" for experimenting with innovative use cases linked to its blockchain infrastructure. This sandbox, which will run from 2023 to 2026, will support 20 projects each year, some of which will involve the use of EBSI by the public sector. In other words, when the closed blockchains of entities (companies, public institutions) are compatible with those of EBSI, then EBSI will benefit by design from the compatibility of its blockchain with those of all other entities linked to this IT infrastructure. EBSI represents a kind of political enterprise blockchain, and could eventually be compatible (subject to political will) with other, more open blockchains[304] . Although public blockchains are currently decentralized, their social adoption is limited due to a lack of legal and political recognition, creating relative competition with EBSI, which enjoys strong political and legal support.

2.3 Blockchain, a technology in the wake of the Internet (Web 3.0)

First and foremost, blockchain technology is just a particular type of electronic ledger. While all blockchains are computer registers, not all computer registers are blockchains. If a register is a generic concept describing the storage of a list of information of the same nature, so too is a blockchain, but in the specific form of a sequenced sequence of blocks of transactions replicated by a multitude of interconnected computers. Indeed, the term "electronic registry" refers to a wide range of technologies designed to store, synchronize and preserve dematerialized records within a computer network. This principle of maintaining an up-to-date record of transactions is not conceptually new, as the first physical, off-line registers date back to around 4,000 BC in Mesopotamia[305] . These physical registers were kept on clay manuscripts or carved in stone, and were used to record and prove transfers of ownership and manage stocks of agricultural crops. It should be noted that this concept of registers also existed in other civilizations in India and South America[306] , i.e. universally. Registers in the form of books and papers have largely declined with the advent of digital technology and the massive dematerialization of information. The notion of decentralized networks also existed before the appearance of man. Indeed, some living organisms, such as fungi, have succeeded in setting up biological networks.

---

part. As part of these dialogues, use case developers can present their business case to receive legal advice from regulators. The law firm Bird & Bird acts as facilitator, setting up a secure interface between developers and regulators and providing legal advice to selected blockchain use cases. Regulatory issues can concern any area of law." "Launch of the European Blockchain Regulatory Sandbox", in *Building Europe's Digital Future*, available at

[304] The EBSI blockchain currently uses a private version (Proof of Authority - PoA) of the public Ethereum blockchain, *v.* Appendix 6, Focus 2 and 3.

[305] DOU Wenyu, "Blockchain, a revolution in e-commerce", August 7, 2018, in *City Business Magazine*, accessed online January 12, 2022.

[306] QUISQUATER Jean-Jacques, *op. cit,* "What alternative models for identity?

decentralized for millennia, making it historically one of the most successful decentralized kingdoms on the planet. So, would decentralization be a guarantee of longevity for a biological network like a computer? If this strategy works in biology (otherwise nature wouldn't insist on reproducing it), can the same be said for decentralized computing? If analogies exist between these biological and decentralized computer networks, it seems that only time will tell. In simplified terms, a blockchain is a vast encrypted digital repository stored on multiple computers in an open or closed computing environment, *i*.e. whose information may or may not be publicly accessible to third parties. A digital register of this kind involves the coming together of three digital components: a social consensus, a common agreement in relation to a given network, and the exchange and interaction of data between Internet users and computers, which automatically communicate information to each other, thus forming an electronic register of transactions. Today, the term blockchain, sometimes referred to by IT experts as decentralized public key infrastructure ("DPKI")[307] , is often misused. It is not easy for the general public to understand because it refers to a variety of different IT and business concepts, which can make it obscure. However, this difficulty can be overcome by a growing number of innovative examples of the use of this technology. It's important to distinguish between the technology itself and the digital applications derived from it. The Internet is a disruptive technology, of which websites represent just one of the possible applications and use cases[308] . By analogy, blockchain technologies are disruptive technologies, of which the Bitcoin blockchain represents just one possible application[309] . Blockchain technologies therefore need to be thought of in context and by use, in order to avoid the risk of confusion between a technology, its many possible computer variants and its many underlying applications.

A blockchain technology is nothing more than an aggregate of computers called[310] nodes - more or less numerous and powerful depending on requirements - which exchange information and data transactions. So it's not so much the hardware infrastructure of this technology that is revolutionary, but rather its protocol and algorithms, i.e. its computer communication mechanisms, often grouped under the terms consensus mechanism or, more abstractly, governance. In principle, these governance mechanisms studied in the Annexes dictate to computers a new and unprecedented way of exchanging reciprocal information. The operation of a blockchain requires each transaction to be independently verified by other computers in the network.

---

[307] PAPGEORGIOU Alexander, MYGIAKIS Antonis, et al, "DPKI: a blockchain-based decentralized public key infrastructure system", June 1, 2020, IEEE Conference Publication, in *IEEE Xplore*. Retrieved June 29, 2022, from

[308] DUSSER Blandine, CLAUDE Hélicia, "Le guide de sensibilisation de la blockchain, pour mieux comprendre cette technologie", in *DGE Report*, April 2022, entreprises.gouv.fr

[309] Bitcoin is the foundation of the blockchain concept and its first monetary and financial application.

[310] V. Appendix 3 (Focus 1 to 3) and Appendix 6 (Focus 1 to 3).

thousands of times to be accepted, i.e. added to the register of transactions already validated. So, unlike centralized servers that confirm transactions in a few hundred milliseconds, a blockchain requires users to wait on average between 10 seconds and 10 minutes for confirmation according to the rules specific to each blockchain. From a philosophical point of view, the emergence of blockchain as a new technological layer dates back to the 1990s, driven by demands from American libertarian movements, sometimes also of anarchic and transhumanist inspiration[311] . The origins of blockchain technology can be traced back to the advent of cryptography and the quest for anonymity. The traditional, centralized approach to servers and their data is currently the most widespread, remaining a mature and appropriate application method for many enterprise use cases. However, this concentration of data and information exchanges on a single machine means that the information base is unusable, or even destroyed, as soon as it ceases to function, for example in the event of hacking or failure of one of its components. To solve this data security problem, the information will be distributed or decentralized[312] , i.e. spread over several distinct machines, but whose information and data exchanges are common, interdependent and subject to mutual computer validation. Validation of each and every transaction on the network is carried out in the form of *blocks*[313] of transactions, and is conditional on acceptance - set by consensus rules[314] - by the computers in this 3.0 computing fabric. The theoretical advantage of a blockchain is to make the probity and transparency of the verification processes taking place on the network visible to all.

At this stage, it seems that the singularity of a blockchain lies in the fact that each computer on the network can respectively validate transaction requests, while simultaneously copying and storing on all the other computers each and every data transaction carried out by all network users. To achieve this, all the transactions validated by each machine are grouped together in successive blocks of transactions, cryptographically linked to each other by consensus: a block chain is formed. Generally speaking, the computers in a blockchain network are fragmented, i.e. they are geographically distributed in different parts of the world. This results in a decentralized registry and transaction history. In this case, the blockchain network no longer requires

[311] BOUSQUET Marc, "Tout savoir sur le Bitcoin et les cryptomonnaies", Ed. du Sens, "un homme augmenté et une liberté absolue de l'humain, libéré notamment du poids étatique grâce à la puissance des machines", in *Dossiers Science Hors-Série*, Nov. 2022, p. 10.
[312] IT doctrine makes a distinction between data distribution and data decentralization. The former distributes data partially, the latter almost totally. This is a distinction of degree, not of kind; *see* Glossary.
[313] A transaction block cannot be altered without affecting the entire upstream and downstream chain. Rectification is so computationally intensive as to be theoretically impossible.
[314] V. Appendix 6, Focus 1.

the intervention of a centralized trusted third party to ensure the validity, continuity and maintenance of the transactions carried out. As explained in Annexes[315] , these connected computers dedicate part of their computing power to validating, recording and maintaining, autonomously and simultaneously, a common log and history of exchanges carried out between users of this decentralized network. It should be stressed that the nature of these information transactions can vary according to the specific purpose of each blockchain: financial transactions (in the form of crypto-assets), contractual transactions (digital contracts), social transactions (electronic voting rights and electronic signatures) and phygital transactions (digital traceability of goods and/or physical products with digital tokens such as NFTs[316]). For reasons of readability and comprehension, this study refers to the term blockchain in its general, mainstream acceptance, except where clarification is required to address certain specific concepts, particularly with regard to certain IT variants represented by the public, private or hybrid blockchains explained below. Since 2020, it should be noted that AFNOR has set up working groups and an optional semantic standard to provide a common vocabulary in French for many of the terms associated with this 3.0 technology[317] . Blockchain technology emerged shortly after the Internet revolution, which implies that it is a form of technological inheritance despite many differences[318] . While the Internet initially advocated free, instantaneous and anonymous access to information centralized on servers, blockchain technology proposes the universal decentralization of data to ensure integrity and sovereign, even optimized, user management over it. To fully understand how blockchain technology has evolved since its first

[315] V. Appendix 3, Focus 1 to 3.

[316] The term refers to "*Non Fungible Tokens"* or "*NFTs",* which, depending on the context, can extend the existence of a physical asset into the digital universe, thanks to cryptographic methods/standards/properties specific to certain blokchains. The simplest way to describe NFTs is to compare them to signed posters of your favorite artist. For example, you like an artist who has created a poster of his latest work. He has just issued 50 copies of this poster with his handwritten signature, so it's a unique series. When you buy an NFT, you buy one of these 50 copies. However, on the Internet, you can always download a copy with just a few clicks. But it's not the one with the digital signature, and it's not the one with the serial number. You're not buying the copyright to his work, but you are buying a copy of the work signed by the artist. Initiated on the Ethereum blockchain in 2015, by 2022 there are three main types of *JNF*: (i) *ERC-20s*, which are fungible tokens, all of the same type for the same smart contract, (ii) *ERC-721s*, each token of which is unique and corresponds to one or more underlying assets, (iii) *EIP-2981s* or more recently *EIP-4907s*, which represent an "NFT standard" for the payment of royalties to authors in transfers between subsequent owners. In 2023, Ethereum developers (including Vitalik Buterin) are expected to propose a new type of NFT: the *"Soul Bound Token (SBT)*", whose purpose is to prove a (revocable) quality by sending *SBT* tokens to an ethereum address. *SBTs* thus play the role of a certificate, the particularity of which lies in their revocability by each issuer: when an *SBT* is sent to an address, only its issuer can revoke it, not its holder and recipient. As a result, an *SBT* could fulfil the same purpose as a *verifiable attestation*, in the knowledge that both can implement *ZKP* and therefore comply with the RGPD. Thus, RGPD and public blockchains are compatible provided that adequate cryptographic mechanisms enable users to retain a high degree of control, transparency and trust over their data.

[317] See the work of the Blockchain Standardization Commission, AFNOR/CN, list of members (Sept. 2022) available at.

[318] Reference is made to the technical standards used, which differ in their implementations although they often have a common origin.

[319] was launched online in October 2008, and[320] went live in 2009, as an underlying Internet application.

2.3.1 A new type of transaction for the emergence of a trusted Internet

Since 2015, blockchain technology has seen growing adoption as well as interest among many players in the public and private sectors[321] . The diversity of these technologies effectively enables new sectoral needs to be met[322] in an accessible, transparent, efficient and automated way. When Bitcoin appeared in 2009, this first reliable application of a cryptocurrency was inseparable from its underlying blockchain technology. It wasn't until 2015[323] and 2016[324] that a conceptual separation of Bitcoin and its blockchain technology emerged in people's minds[325] . From that point onwards, Bitcoin embodied and then demonstrated that it was possible, for the first time in the digital universe, to carry out transactions of unique value and without this value being altered, i.e. systematically duplicated. For example, when someone sends a postcard to another person, that person no longer owns the postcard. When someone sends an e-mail, an image, a message or a document over the Internet, they still own them on their computer or telephone, only a copy is sent to the recipient. This analogy sums up the greatest digital challenge to which Bitcoin[326] has responded: making it possible to carry out online transactions while attributing and embodying a digital rarity by guaranteeing the uniqueness, authenticity and total integrity of the data exchanged. This same cryptographically programmed scarcity thus makes it possible to designate and assume that blockchain technology would enable a new Internet of value. To date, the Bitcoin blockchain also represents the most secure computer system in the world[327] , a source of unprecedented digital trust, notably due to its

---

[319] Bitcoin's "*White Paper*" was published by *Satoshi Nakamoto* on the *metzdowd.com* mailing list on October 31, 2008, *v.* "Bitcoin: A Peer-to-Peer Electronic Cash System", available at

[320] The first transaction block of data on the Bitcoin blockchain, also known as the Genesis block, was created on January 3, 2009 at 6:15 pm.

[321] LITAN Avivah, "Hype Cycle for Blockchain 2021; More Action than Hype", in *Gartner.com*, published July 14, 2021, available online and accessed July 16, 2021; *see* also "The strategic business value of the blockchain market | McKinsey", accessed July 16, 2021.

[322] CARSON, Brant, et al. "Blockchain beyond the hype: What is the strategic business value?" Blockchain beyond the hype: What is the strategic business value?", McKinsey & Company. 2020. Available at

[323] The concept of blockchain, dissociated from its origin (Bitcoin), appeared in 2015 in a Bloomberg promotional article by Blythe Masters a former British executive at JPMorgan Chase bank.

[324] Bitcoin was the first large-scale decentralized computer network, and has given rise to other distributed networks of a similar nature, but operating more or less differently. As the EU Blockchain Observatory and Forum report admits, there was a "before" and an "after" Bitcoin: "Consensus protocols can be divided into two main families [...]: those that existed before Bitcoin, the consensus based on the Byzantine system; those that only exist after Bitcoin, Nakamoto's consensus family", p.51.

[325] To demonstrate this, take a look at the number of searches from 2010 to date (on Google Trend) - for the terms "Bitcoin" and "Bitcoin".
"Blockchain" which possess a similar research trend with regard to their initial indistinguishability (prior to 2015).

[326] V. Appendix 3

[327] DELAHAYE Jean-Paul, "Table Ronde du Cercle du Coin : preuve de travail et écologie", consulted online on August 12, 2021, contribution by Jean-Paul Delahaye, computer scientist, mathematician and professor at the University of Lille: "The calculation that is

anti-fragile characteristic[328] . In addition to the introduction of this new paradigm of digital scarcity, these online transactions are exchanged without necessarily resorting to trusted digital intermediaries, whose main activity traditionally boils down to verifying who sends what, to whom, and how, in return for a significant cost and sometimes accompanied by administrative slowness or even relative management opacity.

Indeed, blockchain technology offers a mathematical and algorithmic trust solution[329] that is in principle accessible, autonomous, sustainable, secure, virtually free and free of geographical constraints. A new digital (crypto)economy of trust, involving a reduced role for centralized intermediaries, seems to be gradually emerging. Because trust is created through transparency, and trust is the oxygen of the digital universe, this algorithmic transparency of blockchain technology needs to be understandable to everyone, not just Web 3.0 developers[330] , as is the case today in most blockchain ecosystems. Author and scientist Aurélie Jean explains that "*trust is a feeling of one human being towards another human being only. Talking about trust in an algorithm introduces the user to a blurred vision of the algorithm's responsibilities*"[331] . While this is particularly true of artificial intelligence algorithms, it must be reversed in the case of blockchain algorithms, where trust is, in principle and by design, more open, accessible and transparent. In anticipation of the next part of this study, corporate blockchains (closed) and public blockchains (open) are two types of blockchain, each with its own advantages and disadvantages. The former are generally private and controlled by one organization or group of entities, while the latter are in theory open to all and controlled by all its users. Enterprise blockchains can offer greater flexibility and control for the organizations using them, making them adaptable for many different uses. Public blockchains also have their uses. They are generally considered more secure than enterprise blockchains due to their structures and the number of stakeholders using them. In addition, public blockchains are used for their crypto-assets, such as bitcoin, because of their ability to reliably manage financial transactions. We observe that blockchain technology is a supposedly decentralized database operating as a computer network in reality organic whose "*effect of*

achieved to include new pages [of transactions] in the Bitcoin blockchain makes it an extraordinary computing object unequalled in the world"; see also the video "Bitcoin Tout Puissant", 1er April 2022 on YouTube, accessed on October 18, 2022, at the following address

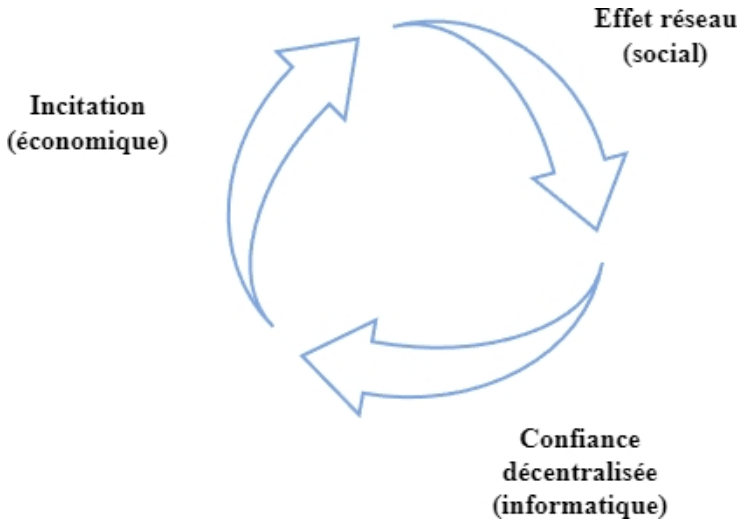
[328] TALEB Nassim, "Antifragile: things that gain from disorder", Random House, 2012, p.430.

[329] LASSEGUE Jean, GARAPON Antoine, "*Justice digitale*", *op. cit*, Ed. PUF, p.153, "It is easy to understand the hope that such a trust machine, a 'machine for producing trust', can raise, given that trust is so central to all human relationships, whether emotional, commercial or political".

[330] Every month, more than 23,000 registered developers are actively involved in public Web 3.0 projects, which corresponds to the total number of current technical employees at Alphabet or Meta, two companies that have been downsizing since the end of 2022, *v*. GitHub

[331] JEAN Aurélie, "*Les algorithmes font-ils la loi?*", in *Humensis*, 2021, *op. cit.* reading position in the book: 69%.

network"[332] and community are two inseparable foundations. Indeed, "*for a blockchain to be decentralized, it is of crucial importance that standard users can operate a node* [of the network] *and that there is sufficient culture* [in this community] *for operating nodes to be a common activity*"[333] . Consequently, it seems possible to illustrate the foundations of an open blockchain according to the following relationships and synergies: an economic incentive generates a social network effect that leads to digital trust, which in turn reinforces this first economic incentive, and so on (*see* next illustration).



In principle, blockchain technology ensures maximum resistance to potential data loss or alteration, as all data exchanged is copied and accessible on every computer in the network, and cannot be altered or deleted without the validation of all or some of the other computers on the same network. Consequently, if a machine is corrupted, it can be isolated without the main network being taken offline or under maintenance for blockchain users. This theoretical resilience of blockchains makes them the tool of choice for companies wishing to foster collaboration both inside and outside their organization, while sharing information and data simply, quickly, securely and immutably. However, the immutability of a blockchain's blocks and transactions closely depends on its level of decentralization, which encompasses, for example, the number and location of dedicated computers, as well as the consensus used for their communication. Thus, it is assumed that only the Bitcoin blockchain today tends towards a degree of pure decentralization, as will be explained later in this study. While decentralization at all costs is not necessarily essential for the use case of digital identity, it is essential for the use case of digital identity.

[332] Term popularized by Robert Metcalfe with his theory of the network effect or "Metcalfe's law".
[333] BUTERIN Vitalik, "The Limits to Blockchain Scalability", accessed online on December 6, 2021.

makes sense with regard to the notion of digital currency, also studied in the second part of this research che.

2.3.1.1 Blockchain, a technology for multiple processes and applications

Blockchain technology can be used to meet a variety of sectoral and business innovation challenges, such as financial services (tokenization of company shares)[334] , transport and logistics (digital traceability of physical goods), public sectors (e-government and augmented institutions), insurance (reliable, transparent and instant insurance) or decentralized digital identity (digital identity of citizens, companies or even connected objects, possibly based on a blockchain)[335] . As Ethereum blockchain founder Vitalik Buterin explains: "There's *plenty of room for blockchain devices that don't just involve* [crypto]*money, and indeed we need more of them*"[336] . Indeed, blockchain houses and aggregates many technological versions, in the same way that the Internet today powers and hosts multiple technologies (artificial intelligence, connected objects) and applications (email, social networks, corporate intranets)[337] . By way of example, many players are already involved in the use of these peer-to-peer and decentralized digital networks, notably in crypto-assets, cybersecurity, traceability of physical goods, virtual reality with decentralized identities (v. Metavers), management of the Internet of Things (IoT/IoT) or the creation of smart contracts (v. AEC) and decentralized autonomous organizations (v. DAO), subjects studied in dedicated sections. It seems important to recognize the variety of possible governance models for each blockchain infrastructure, which can be classified into three categories of infrastructure: those that are open and decentralized, those that are closed and private and centralized, and those that are hybrids of both open and closed and therefore considered semi-decentralized. As a result, there are now as many distributed registry technologies as there are ecosystems and players involved (see Appendices 6 and 7). The great interest shown by many companies in blockchain and its consequent implementation in various applications has led to numerous attempts to adapt this technology. In this respect, some essential clarifications need to be made concerning (i) public-type blockchains, (ii) consortia or hybrid-type blockchains and (iii) private-type blockchains:

---

[334] The *tokenization of* assets involves transposing intrinsic characteristics specific to blockchain technology - security, immutability, speed, transparency, uniqueness - to tangible assets (real estate, movable property) or intangible assets (shares in a company, characteristics of a character in a video game). In concrete terms, it is possible to transfer, immobilize or divide unique virtual representations of these assets.

[335] "It [blockchain] offers [...] an alternative to the equally essential mission of conferring identity (civil status), certifying ownership (land registry) or guaranteeing diplomas.", *op. cit. in* "Justice digitale", Ed. PUF, p.152.

[336] BUTERIN Vitalik, "On Nathan Schneider on the limits of cryptoeconomics", September 26, 2021. *vitalik.ca*. Retrieved April 4, 2022, from

[337] "Blockchain makes it possible to identify, register, and therefore certify identity in a deterritorialized space," *op. cit,* "Digital justice". p.140.

(i) Within a *public blockchain,* all pseudo-anonymous users can, in theory, send, receive and view transaction histories, or even participate in updating the blockchain (notably its consensus algorithm and the process of issuing crypto-assets referred to by the term and concept of "*mining"*)[338] . The user of a public blockchain does not need authorization from a third party in order to carry out operations on the said infrastructure, on which collaboration is free and visible to all. For legal experts, a public blockchain can be seen as a form of contract of adhesion[339] , meaning that a user may or may not adhere to the system as it is designed, and in theory cannot modify it without the agreement of a majority of all blockchain actors. In practice, Bitcoin is the benchmark for public blockchains, and modifying its computer design is an obstacle course[340] .

(ii) Unlike a publicly accessible blockchain, a *consortium* or *hybrid blockchain*, also known as an enterprise blockchain, limits access to data in write mode, but makes it available in read mode. This form of blockchain could be legally understood at the very least as a consensual contract[341] , in which conditions and limitations are negotiated between a small number of duly identified and mutually trusted actors/users. Here, the blockchain system is no longer completely decentralized in IT and/or social terms (*see* Appendix 7), which means that the digital trust attributed to it by its users relies on one or more public and/or private trusted third parties, generally a group of institutions and service providers. In a hybrid blockchain, only members of the group of authorized persons can participate in the consensus-building process (governance). The history of the blockchain can be made accessible either to all users, or to one or more specific groups. By way of illustration, the Hyperledger Indy blockchain[342] achieves optimal consensus when 25 nodes and computers are operational (which is very few compared with public blockchains), and at least 8 nodes out of 25 must be functional to ensure the relative IT resilience of the deployed blockchain[343] .

---

[338] V. Appendix 6, Focus 1.

[339] Art. 1110 al. 2 of the French Civil Code: "A contract of adhesion is one which includes a set of non-negotiable clauses, determined in advance by one of the parties".

[340] V. Appendix 3, Focus 1 to 4. While it is mathematically impossible to falsify transactions on Bitcoin, one potential vulnerability lies in its community of volunteer developers, who have been proposing numerous software updates to the protocol (*Bitcoin Improvement Proposal - BIP*) since 2009. A malicious actor could thus attempt to submit a malicious BIP to the community of volunteer developers, which, if accepted, could introduce programmed flaws ("back doors") into the protocol. It should be noted that this type of attack is mainly the result of political and theoretical conjecture, and is very rarely seen in practice.

[341] Art. 1109 of the Civil Code, in the version in force since October 1er 2016, which states: "A contract is consensual when it is formed by the sole exchange of consents, whatever the mode of expression (...)".

[342] Hyperledger Foundation. Hyperledger Indy. Retrieved September 29, 2022, from

[343] V. *Learningthings.online*, "Introduction to Hyperledger Sovereign Identity, Blockchain Solutions", accessed online on 14/10/2021.

In 2022, this same infrastructure (Hyperledger), which is massively used for decentralized digital identity use cases, was partially criticized for its lack of decentralization[344] : "*it is interesting to note [...] that the ideal point is 25 nodes - robust, capable of surviving the failure of eight nodes, but fast enough to support the expected number of write transactions on the network - of the order of hundreds of transactions per second*". These technical explanations are explained in greater depth in a section dedicated to the current challenges of blockchain technologies. However, since the end of 2022[345] , fifteen major players in the insurance sector have decided to put an end to their joint blockchain consortium project, mainly due to a lack of knowledge and market opportunities. Similarly, another consortium blockchain created in 2017 has announced that it will cease operations in November 2022[346] . Indeed, it seems extremely difficult, if not impossible, to get ever more players in a sector and a hybrid blockchain to collaborate over a long period of time (long-term productivity gains are offset by governance that is sometimes deemed too complex compared with traditional, bilateral collaboration methods)[347] .

(iii) In the case of a *private blockchain,* user information and authorizations are fully framed, and are neither free as in the case of public blockchains, nor partially decided by a restricted consortium of players, as in the case of hybrid blockchains. In principle, a private blockchain is developed by a single player who wishes to retain control. In a private blockchain, the transaction history is no longer transparent to third parties, but only accessible to the administrator (usually the only one) of the blockchain in question. Authorization to update the blockchain and create transactions is thus limited and controlled by this same actor, making a private blockchain a form of unilateral contract for its users under the provisions of the French Civil Code[348] . This absolute control by a totally centralized third party means that modifications to the software are simpler and quicker to make. However, certain characteristics (attributable to public and sometimes consortium blockchains) such as immutability and decentralization of operations

[344] YOUNG Kaliya, "Being 'Real' about hyperledger Indy & Aries / Anoncreds", September 7, 2022, in *Identity Woman*. Retrieved September 12, 2022, from

[345] VIVIANI Mathieu, August 12, 2022, "Blockchain : une quinzaine de grands assureurs internationaux jette l'éponge", in *Les Echos.* Available at

[346] "IBM, Maersk shutter shipping blockchain TradeLens", November 30, 2022, in *Ledger Insights - blockchain for business*. Available at

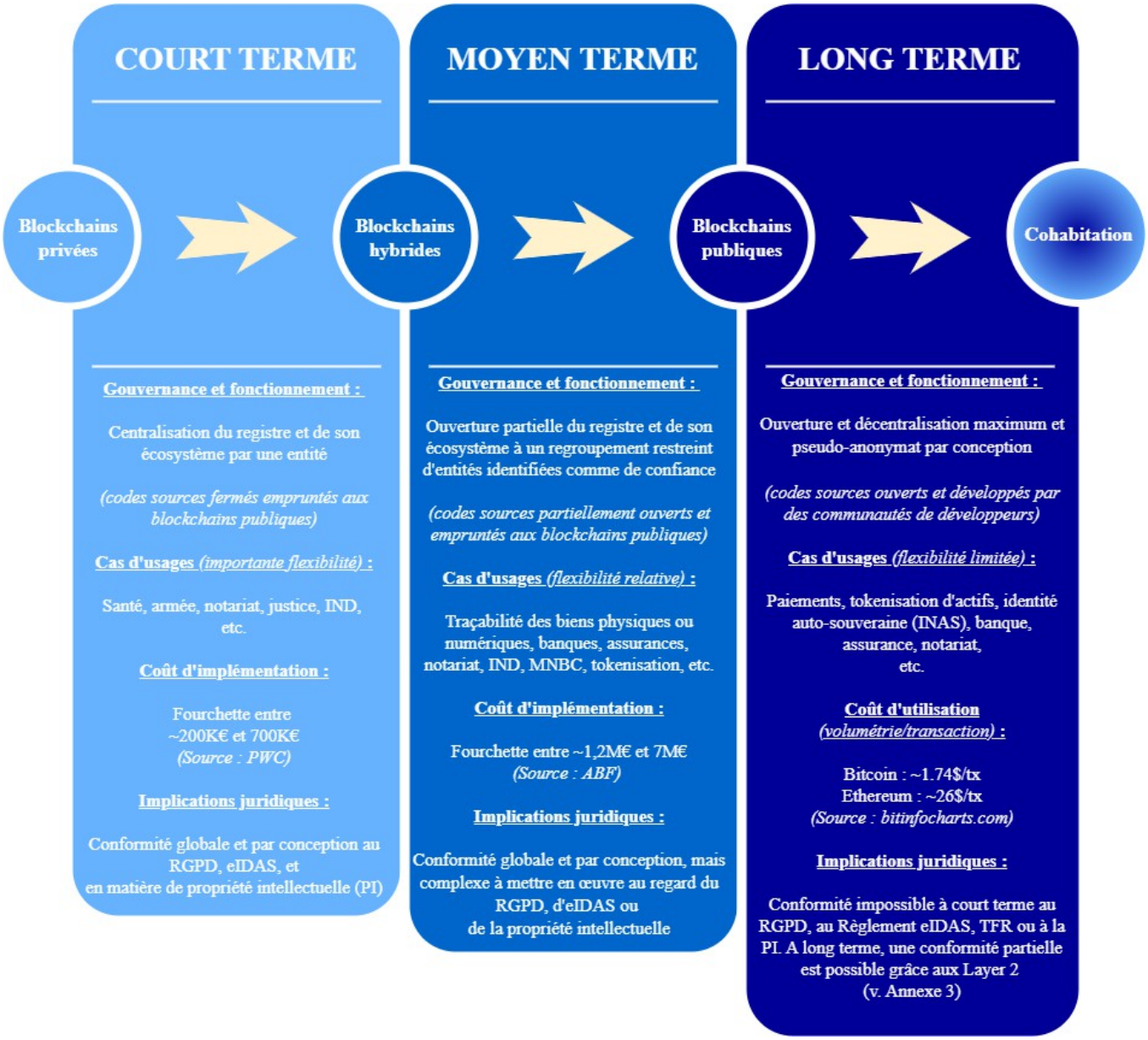
[347] "According to a study conducted at the end of 2019, the era of private blockchains may even be coming to an end, and the future belongs to private platforms built on top of public blockchains, a kind of overlay that some companies are already offering. (...) The very latest public blockchain solutions enable companies to exploit public blockchains, while guaranteeing data confidentiality. It would seem that the future lies in securing public blockchains", *op. cit. in* "Tout savoir sur le Bitcoin et les cryptomonnaies", p.15.

[348] Art. 1103 of the Civil Code, in the version in force since October 1er 2016, which states "legally formed contracts take the place of laws for those who have made them".

can be called into question, implying less confidence in these registers for users wishing to use open, decentralized systems. Finally, it should be noted that while a private blockchain is in reality a grouping of centralized servers under the authority of a single entity, with only the IT and algorithmic foundations modified in comparison with conventional servers, such a system is assumed to be legally compliant here, since its administering entity is generally so from the outset (legally-formed company, etc.).

When a blockchain is public, private or hybrid, the computer consensuses used are not necessarily the same, as demonstrated in a dedicated Appendix[349] . Each type of blockchain therefore has its own advantages and disadvantages, which have greater or lesser effects depending on the field(s) of application. In this sense, a private blockchain may be destined to become a consortium blockchain, but a consortium blockchain is not destined to become a private blockchain. In both cases, neither a private blockchain nor a consortium blockchain seems to be in a position to become a public blockchain, as pre-existing public blockchains benefit from a network effect, greater technical experience and trust, and are assumed to be unrivalled in the long term[350] . This more or less open nature of each type of blockchain is reminiscent of a confrontation well known to the pioneers of the Internet, that of proprietary software versus free software, which is studied in a dedicated section[351] . Some specialists in the French blockchain ecosystem believe that private or hybrid blockchains, with no associated universal or artificial token, *provide* "(...) *only marginal operational gain at the cost of often very high costs* (...)"[352] . While this may be relevant to the financial sector, it does not necessarily apply to the digital identity market. Indeed, unlike these sectors, financialization through virtual tokens or crypto-assets is not yet envisaged in the short term by the majority of digital identity players.

[349] V. Appendix 6, Focus 1 to 3.
[350] BABEAU Olivier, President of the Institut Sapiens and Professor of Management Sciences at the University of Bordeaux, explains that "The network effect is the new paradigm of monopoly" in *Le nouveau désordre du numérique : comment le digital fait exploser les inégalités*, Ed. Buchet-Chastel, 2020, 267p.
[351] V*, infra,* II, Title 1, 1.5.3.1
[352] STACHTCHENKO Alexander. January 11, 2022. "Survival manual in the jungle of anti-Bitcoin clichés" (long version accessed online 12/01/2022).



The diagram above enables us to assess the suitability of each type of blockchain for different use cases over time. First, it is possible to assume that private and hybrid blockchains are merely temporary technological versions intended for use until public blockchains can address some of the computational, social and legal challenges studied throughout this research. For decentralized, open and public protocols, the hope of this scenario is to meet these challenges through the future and successive implementation of so-called second-layer protocols ("Layer 2 - L2")[353] , solutions that are currently more centralized than decentralized. Thus, the public versus private blockchain debate would no longer be relevant if these underlying implementations (L2) were to become a reality, as these blockchains would

[353] V. Appendix 3, Focus 4.

In the future, the still decentralized public sector will be interconnected to protocols that meet these challenges. Indeed, the greater semi-centralization of these relay protocols would make possible a certain flexibility enabling companies to participate in these open protocols, in legal and energy compliance (see Appendix 6) corresponding to societal expectations. Pending this hypothetical reality, in the short and medium term, a company has no choice but to favor private and hybrid blockchains for certain domains, as public blockchains currently offer no viable solutions to the following issues they have been facing since 2015 on an IT level:

(i) Is the response time per blockchain transaction sufficient (on the order of a millisecond, as for a server, or several seconds or minutes, as for a public blockchain)?

(ii) Is the cost per transaction reasonable (virtually zero for a server, but very high on a public blockchain)?

(iii) Does the blockchain accept sufficient load capacity in the event of heavy demand on the network by its users (is a redundancy system envisaged)?

(iv) Is it possible to make the necessary effort to ensure that this IT system complies with the law, and to what extent?

In October 2022, Google launched a new solution called "*Blockchain Node Engine*"[354] which offers a fully managed blockchain node hosting service for organizations wishing to develop sector-specific (partially decentralized) use cases. Although this solution may be of interest to organizations such as the ABF or EBSI mentioned above, it seems to contradict the objective of European sovereignty and its Regulations (Data Act, eIDAS, studied later). In practice, Web 3.0 companies that need dedicated nodes can relay transactions, deploy smart contracts and read or write data from a blockchain, with the reliability, performance and security they expect from the computing and network infrastructure attached to the Google Cloud service. Ethereum[355] will be the first public blockchain supported by this new service, enabling developers to provide turnkey, fully managed Ethereum nodes with secure access to the blockchain. It should be noted that another American company, Amazon, has been offering a competing service since 2019[356] . In the long term, we assume that certain public blockchains, such as Bitcoin or Ethereum, will have the technical capacity to host certain use cases in the digital identity sector (see INAS). Overall, then, blockchain technology should continue to develop and prosper, in an environment that

[354] ZAVERY Amit, TROMANS James, "Introducing Blockchain Node Engine: fully managed node-hosting for Web3 development", October 27, 2022, in *Google Cloud Blog*. Available at

[355] V. Appendix 6, Focus 2.

[356] "Amazon Managed Blockchain Pricing", in *Amazon Web Services (AWS)*, Inc. Retrieved October 27, 2022, from

is progressively becoming digitalized, and in which the notions of digital dependency and trust concern more and more companies, institutions and citizens. However, since 2021, many concerns have resurfaced regarding the energy consumption of blockchains. While private and hybrid blockchains consume less energy than public blockchains such as Bitcoin, because they have known and identified validation nodes which avoid the mathematical calculations required to verify the authenticity of an actor and validate a transaction, it is important not to misjudge public blockchains without carefully examining the real energy impacts of their computing activities[357] . These impacts may be more complex and surprising than they appear. Finally, this study only evokes certain use cases relating to blockchain technology and digital identity. It does not aim to provide a segmented analysis by use case, but rather to provide a cross-sectional view of some of its applications with regard to the many issues linked to centralized and decentralized digital identity.

2.3.1.1.a Crypto-assets

Scientists such as the famous American economist Milton Friedman anticipated the era of virtual currencies as early as 1999[358] . Referred to as crypto-currencies or crypto-assets, and as digital assets in our positive law[359] , these words, which are almost commonplace today, encompass a multitude of virtual *tokens* backed by open blockchains. Initially, these virtual objects were created to protect blockchain infrastructures from attacks by spammers seeking to overload them with multiple transactions. However, due to their fluctuating value, influenced by factors such as token supply and demand, the underlying IT infrastructure and massive marketing campaigns, these digital tokens have gradually become particularly speculative objects of use. In other words, as the aforementioned founder of the Ethereum blockchain, Vitalik Buterin, explains:

"*crypto economics is about trying to reduce the risks associated with social trust by creating systems in which we introduce explicit economic incentives for good behaviour and economic penalties for bad behaviour*"[360] while

[357] V. Appendix 6, Focus 1.

[358] KRYPTOSPHERE®, "Milton Friedman predicted the air of crypto-currencies in 1999!", 2018, accessed online January 13, 2022.

[359] Loi n° 2019-486 du 22 mai 2019, dite PACTE, relative à la croissance et à la transformation des entreprises, for a definition of digital assets, *v.* art. L.54-10-1 of the CMF: "1° The tokens mentioned in article L. 552-2, excluding those fulfilling the characteristics of the financial instruments mentioned in article L. 211-1 and the savings bonds mentioned in article L. 223-1; 2° Any digital representation of a value which is not issued or guaranteed by a central bank or public authority, which is not necessarily attached to a legal tender and which does not have the legal status of a currency, but which is accepted by natural or legal persons as a means of exchange and which can be transferred, stored or exchanged electronically".

[360] "Governance, Part 2: plutocracy is still bad", March 28, 2018, in *vitalik.ca*. Accessed April 1, 2022, at

others evoke the tyranny of crypto-assets[361] . As suggested by a group of legal specialists on the subject, the term crypto-assets (written here with a hyphen) is preferred throughout this research[362] . While these multiple names and their difficulties of apprehension seem to show the applicative potential of this sector, digital assets are introduced in article L.54-10- 1 of the French Monetary and Financial Code: "*any digital representation of a value which is not issued or guaranteed by a central bank or by a public authority, which is not necessarily attached to a legal tender and which does not have the legal status of a currency, but which is accepted by natural or legal persons as a means of exchange and which can be transferred, stored or exchanged electronically*"[363] . Digital assets thus appear to be a separate asset class from other existing financial instruments. In EU law, a crypto-asset is qualified by Article 3(1)(2) of the MiCA Regulation (studied in a later chapter) currently being adopted, as "*a digital representation of a security or right which uses cryptography for its security and is in the form of a coin or token or any other digital medium which can be transferred and stored electronically, using distributed electronic ledger technology or any other similar technology*"[364] . Until 2019, crypto-assets were almost exclusively perceived by national legislators as instruments of fraud, money laundering and terrorist financing. It was only after Facebook unsuccessfully attempted to issue its own stable crypto-asset, originally called the "*Libra*", that European lawmakers decided to seriously consider this 3.0 universe[365] . Although France is lagging behind in the adoption of crypto-assets, both by institutions and the general public, as revealed in 2022 by an international study[366] , the fact remains that French lawmakers have demonstrated, since 2019, a significant capacity for anticipation and legal innovation concerning them, to the point of inspiring EU law from 2020 onwards. In fact, as early as 2018, it was Swiss legal doctrine that established a precise and initial taxonomy specifically dedicated to the different types of crypto-assets (see below)[367] . Widely adopted by regulators around the world, this doctrine from the Swiss Financial Market Supervisory Authority (FINMA)[368] a

---

[361] LARMAGNAC-MATHERON Octave, philosopher, "La tyrannie des cryptomonnaies," published January 11, 2022, in. *Philosophie magazine*, available at

[362] BOUILLET-CORDONNIER Ghislaine et al. " La Finance Numérique, Aspects juridiques et fiscaux du crowdfunding et des cryptoactifs", Ed. EFE, 2021, "Le terme actif numérique inséré dans le règlement général de l'AMF est à bannir au profit de celui de crypto-actifs. [...] the term [digital asset] is a source of confusion", p.146 (n°395), and "[...] the notion of crypto-assets has become heterogeneous, encompassing very diverse realities. As a result, the legal definition previously mentioned has become blurred", and see also "Monnaies, banques et finance: vers une nouvelle ère crypto, un enjeu de souveraineté et de compétitivité économique, financière et Monétaire", in *Rapport de l'Assemblée nationale*, *op. cit.* p.11.

[363] Art. L 54-10-1 of the CMF, Légifrance consulted on July 28, 2021 and *see* also II, Title 2, 2.4 *below.*

[364] RADLEY-GARDNER Oliver, BEALE Hugh, ZIMMERMANN Reinhard (eds.), freely translated from English, Fundamental Texts On European Private Law: Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, online, Hart Publishing, 2016, accessed March 4, 2022, p.59 and see *infra*, I, Title 2, 2.5

[365] See infra, II, Title 2, 2.4

[366] Bitstamp, "Crypto Pulse Report", 2022, pp.7-11. Available at

[367] BOUILLET-CORDONNIER Ghislaine, LANGLOIS-BERTHELOT Thibault, "Tour d'horizon du droit financier Suisse", online, *op. cit*. Ed. EFE, 2021.

[368] Acronym for Swiss Financial Market Supervisory Authority. V. Dictionary of acronyms

This nomenclature has subsequently infused many legislative frameworks, notably in Europe and the United States. This nomenclature distinguishes[369] :

(i) *Payment tokens*

This first type of token characterizes the digital assets that are regularly in the news. They can be defined as new ways of storing value, exchanging and paying quickly, securely and without intermediaries or borders. They enable the purchase of goods or services, but confer no specific rights vis-à-vis a third-party issuer: they are not characterized as securities. In the United States, this type of token (bitcoins, ethers) will be massively adopted by merchants over the next five years, according to a report by Deloitte in collaboration with Paypal[370] .

(ii) *Utility tokens*

This type of token offers a posteriori access to a specific product or service (access to a 3.0 application and/or a physical asset), when funds are raised in crypto-assets to develop a good or service. These tokens can supposedly be used by early investors to benefit from highly advantageous benefits and quid pro quos (such as discounts, voting rights). This type of utility token is intended for use within the ecosystem and project developed by the issuing company.

(iii) *Security tokens (STO*)

Investment tokens represent a new class of financial assets to which profit rights are attached. They are generally based on tangible or intangible assets. As a result, offers of investment tokens are in part easily subject to regulation, since they represent the digital extension of legal acts (allocation of company shares, voting rights). With the aforementioned intrinsic advantages of blockchain technology, investment tokens digitally reproduce tradable or non-tradable securities (shares, bonds, derivatives, company shares, profit-sharing, interests) on the primary or secondary market. Consequently, Swiss law considers investment tokens to be securities.

In practice, many companies in the blockchain technology sector use one or more tokens that can characterize both payment, utility and investment tokens. In these cases, the qualification and legal framing of the latter become more complex to

[369] FINMA, "Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO)", February 16, 2018, p.7, available at.

[370] CASTRO TANCO Claudina, "Merchants getting ready for crypto Merchant Adoption of Digital Currency Payments Survey Prepared in collaboration with PayPal", free translation from English "Around 85% of merchants surveyed expect crypto-asset payments to be ubiquitous among their companies' suppliers", pp.5-8, available online at.

interpret for regulators. Crypto-assets are revolutionary because, among other things, they enable the established order to be transformed, sometimes overturning it[371] . As this study suggests for bitcoin[372] , these cryptographic assets enable their owners to establish or re-establish relative financial freedom, thanks to transparent algorithmic and mathematical mechanisms. This financial trust 3.0 is based on the idea that when every transaction is verifiable on a public blockchain, it becomes simple to trust people and engage in *phygital* interactions. This new breath of emancipation implies a new, more decentralized and peer-to-peer conception of our social interactions. While this new cultural trend and social movement entails certain risks (loss of funds, scams) and limitations (relatively complex management of cryptographic keys), it is nevertheless a question of overcoming certain conservative reflexes in an attempt to understand and frame this technology, which is often compared to the advent of the Internet. It seems that the market will probably end up convincing and changing mentalities, a fact that is already visible. The evolution of physical money towards cryptocurrency is thus an underlying need of the Internet. While it has to be admitted that the French strategy for the supervision and adoption of crypto-assets is politically, legally and economically conservative, not least because of a banking lobby that is often unfavorable to this new asset class[373] , this observation should not be transposed to players in the decentralized digital identity market, as the workings of this sector are not fundamentally financial. Although almost 70% of blockchain technology applications in 2019 concerned financial use cases[374] , other use cases are gradually emerging, as one of the eight co-founders[375] of the Ethereum blockchain pointed out in 2021 "*it's time to go beyond finance applications*"[376] . As explored below, decentralized identity will eventually become as important for digital currency as it is for digital identity. In other words, there will no longer be a need for multiple apps and digital wallets to manage the attributes (cryptographic keys) of one's identity, relationships and (cryptographic) money[377] . Thus, the culture of crypto-assets[378]

---

[371] MALABOU Catherine, "Les cryptomonnaies remettent en cause l'idée même d'Etat", philosopher and signatory of "la déclaration d'indépendance des cryptomonnaies", published October 6, 2020, in *Philosophie Magazine.*

[372] V. Appendix 3, Focus 4 to 6.

[373] PERSON Pierre, former Member of Parliament, June 8, 2022, "We underestimate the weight of the banking lobby", "In France, the strength of the banking lobby should not be underestimated. It's a fact that part of the senior civil service has close ties with the French banking sector. This is not a question of direct or individual economic interests, but rather of an inability to imagine a different world when one's entire career has been spent between these two environments. This is not conspiracy theorizing, which I abhor. [...] The latter are not fundamentally opposed to cryptos, but this decentralized logic is contrary to their intellectual construction", consulted on June 9, 2022, at the following address. To illustrate other remarks *v.* also "Droit de la finance numérique, blockchain, aspects fiscaux", EFE Edition, 2021, pp.147-151 (n°397- 402) ⟨hal-03473371⟩.

[374] *Op. cit. v.* public data from the blockchainforgood.fr website.

[375] The Ethereum public blockchain and its ecosystem was initiated by eight co-founders, of whom Vitalik Buterin is the most emblematic contributor to date. These people are clearly known and identified, unlike the founder(s) of the Bitcoin public blockchain.

[376] BUTERIN Vitalik, on *Cryptoast*, online, 2021, accessed August 4, 2021.

[377] "Money didn't have a smell, but now it has a trace, and it's indelible", *op. cit.* GARAPON Antoine, LASSEGUE Jean, "Justice digitale.

[378] "Pas vos clés [cryptographiques], pas votre argent [cryptographique]", freely translated from the English expression popular in the crypto-asset world "not your keys, not your coins".

is based on financial autonomy and the autonomous management of financial assets, and we assume that the ethics and culture of identity autonomy claimed by self-sovereign digital identity could be expressed by the mantra "not the owner of your identifiers (DID), not the owner of your identity"[379] . While it is possible today to distinguish between crypto-asset wallets[380] , and the decentralized digital identity wallets (PIND) studied under the second heading of our study, it is likely that in the medium term these two types of applications and digital wallets will merge to become one. With regard to crypto-asset services, the forthcoming EU-wide application of the MiCA Regulation[381] will impose a new legal rule, the

The MiCA "*travel rule*"[382] , some of whose requirements (legal and IT) could constitute the standards for decentralized identity, which everything points to as a suitable solution in this area. The MiCA Regulation stems from the fact that crypto-assets were not covered by European Union financial regulations, as this lack of rules applicable to services linked to these assets could expose consumers and investors to certain risks. It aims to support innovation and fair competition by creating a framework for the issuance and provision of services linked to crypto-assets. Furthermore, the subject of "stable" crypto-assets, referred to as "*stablecoins*" below, represents an additional legal challenge both for their consumers and users, and for the European Commission and its member states, whose monetary sovereignty may be called into question[383] .

2.3.1.1.b Electronic and cryptographic signatures

An electronic signature can be defined as a set of computer, mathematical and software methods and constructs[384] that aim to attest to the integrity of a digital document or object, while authenticating its author[385] . Thanks to electronic signatures, it is now possible to sign legal documents online and carry out (crypto)financial transactions,

---

[379] This mantra is loosely based on the previous one, and helps us understand the importance of people controlling their digital identifiers (DIDs).

[380] A crypto-asset wallet represents a mobile application enabling interaction (buying, selling, sending, receiving) with one or more crypto-assets depending on the application's functionalities. V. Appendix 3.

[381] Proposal for a Regulation of the European Parliament and of the Council on crypto-asset markets (MiCA), amending Directive (EU) 2019/1937.

[382] COMPANI Sarah, "MiCA Regulation: the beginnings of a new European financial paradigm", December 8, 2021, "[...] any service provider on crypto-assets will be required to identify the issuer and the actual recipient of each transaction, Numerous questions of interoperability of information exchange mechanisms arise and it is not impossible that an international information exchange standard specific to transfers on blockchain will see the light of day in the coming years, particularly in the context of reflections in relation to the implementation of the travel rule", in *Village de la Justice*. Consulted online on March 7, 2022, see also *infra,* I, Title 2, 2.5.1

[383] See *infra*, II, Title 2, 2.4.

[384] "Lexique de termes juridiques 2017-2018", "[...] consists in the use of a reliable identification process guaranteeing its link with the act to which it is attached", consulted online on October 28, 2021, p.1904.

[385] Decree no. 2022-1620 of December 23, 2022 (JO of 24) amended Article R123-5 of the French Commercial Code concerning the requirement for an electronic signature quality certificate, in particular for RCS amendment and deletion formalities: "the identifier of the declarant by a means of electronic identification corresponds to a substantial or high level of guarantee included within the electronic identification scheme notified under Article 9 of Regulation (EU) No. 919/2014 of July 23, 2014 on electronic identification (...) associated with a simple electronic signature, is equivalent to an advanced electronic signature based on a quality certificate".

sometimes without revealing his or her civil identity[386] . In this respect, a distinction must be made between, on the one hand, the electronic signature, which refers to a dematerialized handwritten signature within the meaning of the provisions of the French Civil Code (initially linked to a person's pivotal identity)[387] , and, on the other hand, the pseudo-anonymous cryptographic signature, discussed below, which does not necessarily reveal the pivotal, civil identity of its signatory. The case discussed below implies that the person signing does not need to reveal his or her civil identity, but it is essential that his or her identifier and cryptographic signature are linked in a certain way to enable identification by the recipient. Electronic signature systems based on asymmetric encryption algorithms, which first appeared in 1975[388] , have been in widespread use for many years now. Each user has two encryption keys (two sequences of numbers and letters), randomly generated using mathematical algorithms: a public key and a private key. They are uniquely associated and derived from each other[389] and are unique to each user. The key that enables sensitive operations to be carried out (decrypting an encrypted message, electronically signing an encrypted message) is called the private key. The other, public, key is used for public operations, i.e. verifying the encryption of a message or its signature by the sender. In this way, a message encrypted with a private key from such a system can only be decrypted with the corresponding public key, and vice versa. Any public key is an element that can be shared and known by all, while the private key must remain secret and never be shared with a third party (at the risk of identity theft). When this type of algorithm is used to generate an electronic signature, these two keys are used to verify the authenticity and integrity of each message. This native cryptographic signature functionality is present in all blockchain systems and relies on[390] pseudo-anonymity, which will be explored further below, as well as on[391] computer decentralization to a greater or lesser extent, depending on the purposes pursued by these infrastructures. Not all[392] electronic signature 2.0 solutions use asymmetric cryptography mechanisms. Applied to blockchain technology, these various cryptographic and online identification mechanisms guarantee the authenticity and integrity of the data sets or documents to which electronic signatures are associated. Here, asymmetrical cryptography guarantees the origin and initiator of a document's electronic signature. A blockchain registry enables the existence of a document to be verified.

---

[386] This pseudo-anonymity allows an electronic signature compatible with the rules of the RGPD*, see infra,* I, Title 2, 1.4.1

[387] Art. 1366 of the Civil Code in the version in force since October 1er 2016, which states: "Electronic writing has the same probative force as writing on paper, provided that the person from whom it emanates can be duly identified and that it is drawn up and stored in conditions likely to guarantee its integrity".

[388] V. "Asymmetrical encryption", May 31, 2022, in *IONOS Digitalguide*. Available at

[389] In essence, this mechanism works in such a way that a *private key* is derived from a *master public key* accessible to all: this system thus makes it possible to prove both one's ability to sign (private key) and one's membership of a key derivation scheme (public). For example, it is possible to provide digital identities to a group of people identified by their *master public key*.

[390] See I, Title 2, 1.4.1 *below.*

[391] See I, Title 2, 2.1.3 *below.*

[392] Reference is made to electronic signature services already used by lawyers, such as HelloSign, DocuSign, Dropbox Sign, etc.

pseudonymous proof of this signature, thanks to the transaction in which its digital fingerprint is embedded. This dual key mechanism enables the owner of a private key to digitally sign a transaction request in order to prove that he or she is the originator, and a verifier to ascertain the authenticity and ownership of said signature inscribed directly on a blockchain, which may be open or closed. In this way, blockchain technology provides an intrinsic means of electronic signature, which may or may not be associated with other identification or electronic signature mechanisms from centralized and/or decentralized digital identity systems.

In EU law, the regulatory framework applying to electronic signatures comes under the eIDAS Regulation (studied in the second heading of this research), which partially came into force in 2016[393] . It stipulates that "*the legal effect and admissibility of an electronic signature as evidence in legal proceedings may not be denied on the sole ground that the signature is in electronic form or that it does not meet the requirements of a qualified electronic signature*", which ensures that it is admissible in legal proceedings in the same way as a handwritten signature. To provide a practical framework for the diversity of contractual needs, the eIDAS Regulation distinguishes between three levels of electronic signature: simple[394] , advanced[395] and qualified[396] . In the light of these three possible levels of digital signature, it is considered that a digital signature on blockchain is equivalent to a simple signature whose legal admissibility in terms of proof is possible[397] . Moreover, articles 25 and 27[398] of the aforementioned Regulation reaffirm that all electronic signatures have legal value within EU countries, a principle which de facto includes blockchain technology, whose technical reliability is presumed to be high (only in the case of hybrid or private blockchains within the meaning of eIDAS-2[399] , which is examined below). In France, the legal framework does not provide for either legal recognition or specific legal provisions for electronic signatures based on a blockchain. Electronic writings have probative value as long as the persons from whom they emanate are identified, and the writing is established and authenticated.

[393] Regulation (EU) No 910/2014 of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, accessed July 28, 2021. *See* also *infra*, II, Title 1, 2.1.1.1.
[394] *Ibid.* Art. 3-10: "data in electronic form, which are attached to or logically associated with other data in electronic form and which the signatory uses to sign".
[395] *Ibid.* Art. 26: "An advanced electronic signature must be uniquely linked to the signatory; allow the signatory to be identified; have been created using electronic signature creation data that the signatory can, with a high level of confidence, use under his exclusive control; be linked to the data associated with this signature in such a way that any subsequent modification of the data is detectable".
[396] *Ibid.* Art. 3-10: "an advanced electronic signature which is created using a qualified electronic signature creation device, and which relies on a qualified electronic signature certificate".
[397] In this respect, the "monjuridique.infogreffe.fr" website offers a Register of dematerialized securities movements based on a private blockchain, consulted on April 11, 2022, *see* the following address and see also *infra*, I, Title 2, 2.8.
[398] *Ibid.* Recital (27), "this regulation should be technology-neutral. The legal effects it confers should be obtainable by any technical means, provided that the requirements laid down in this Regulation are met".
[399] See *infra*, II, Title 1, 2.1.1.1.a

stored under conditions that ensure its integrity[400] . While in practice it might be possible to consider that a digital signature on blockchain (public key/private key) represents a minimal technical association and therefore a sufficient means of identification in its own right, this consideration may nevertheless raise certain complications: (i) when the party against whom a third party intends to prove obligations does not wish to disclose its public key, or (ii) if a public blockchain does not benefit from the aforementioned presumption of reliability. In view of these factors, we believe that two types of situation can be envisaged, the first offering a presumption of reliability and the second offering no certainty at all:

(i) A qualified trusted third party provides a secure electronic signature function linked to a private or consortium blockchain to ensure a presumption of reliability.

(ii) A user, without the help of a trusted third party, would decide alone on the end-to-end management of his or her digital identity. Decentralized or self-sovereign digital identity, for example, would be considered as a simple means of proof, i.e. left to the sovereign discretion of the judge, without benefiting from a presumption of reliability and pending application of the proposed amendment to the eIDAS Regulation[401] .

Ultimately, the recognition of decentralized digital identity (IND)[402] and blockchain technology as reliable legal proof will only be possible if the eIDAS-2 Regulation allows it. This issue is addressed in detail in a separate section. Recognition of these 3.0 electronic signature mechanisms, in line with current legislation, requires the convergence of multiple factors, starting with the (presumed native) IT interoperability of these solutions, right through to their political and legal recognition at national or even EU level. With the arrival of these solutions, third-party certifiers will simply be able to connect to any substantial or strong authentication service based on a decentralized digital identity solution. They will then be able to retrieve a person's legal identity online, certify it and finally proceed with an advanced electronic signature.

[400] We note here the imperative need to ensure the durability of the media (digital identifiers), and their verification mechanisms. In this case, a blockchain (private or consortium) could be used to meet the requirements of preservation and integrity.
[401] See *infra*, II, Title 1, 2.1.1.1.
[402] See *infra*, II, Title 1, 1.1

2.3.1.1.c Peer-to-peer (P2P) network and distributed storage

Peer-to-peer" (hereinafter "P2P") is a type of network architecture in which computers or devices connect directly to each other without the need for a central server. This means that each device on the network acts as both client and server, enabling users to share resources and information directly with each other. This differs from a conventional client-server computing architecture and relationship, in which all network devices are either clients requesting information from a server, or servers providing information to clients. P2P networks are often used for file sharing and other types of online collaboration. They are also used by many blockchains. Even today, the concept of storing data on a blockchain is regularly discussed[403] . However, storing data on a public blockchain is generally expensive (around $100 per gigabyte of storage, depending on the period[404]). From an IT point of view, we need to distinguish between data storage on a distributed system and storage on a decentralized register (blockchain). The first process involves fragmenting (dividing into several digital footprints) the information to be shared, then distributing and distributing it to users' computers, who can then automatically reconstitute it on a peer-to-peer basis (without intermediaries) to obtain complete data such as documents, images or videos. The second system, on the other hand, cannot store large volumes of data due to its prohibitive economic cost. Contrary to popular belief, a blockchain is not an information storage technology, as only simple cryptographic proofs of limited size can be embedded in it, unlike distributed storage networks. Such software and mechanisms for sharing data directly between users' computers are not new; they've been around since the early days of the Internet. They raise a number of legal issues, particularly in terms of liability and intellectual property, as some of these software programs and protocols are not only distributed, but also entirely decentralized, thanks to blockchain technology[405] .

While blockchain and distributed ledger technologies are based on similar concepts as computationally distributed networks (without central authority), this similarity should not lead to confusion: while the blockchain shares a record of continuous transactions between all its nodes[406] , a distributed ledger differs in being a peer-to-peer file-sharing system that sequences information into a multitude o f named digital footprints, the

[403] "Blockchain-based application protocols function like the BitTorrent protocol in many respects, although they do not rely on centralized trackers or distributed hash tables to coordinate network activity," *op. cit.* "Blockchain and the Law", in *Harvard University Press*. Kindle ed. Location 976 of 7004.
[404] OMAAR Jamila, "Forever Isn't Free", in *IPDB Blog* [online], published July 19, 2017, accessed July 29, 2021.
[405] Reference is made to the Ordinnals project, which enables information of all kinds to be anchored in a completely peer-to-peer and decentralized way, directly within the blocks of the Bitcoin blockchain.
[406] V. Appendix 3 & 6

The "*hash*" function[407] enables users to search for and reify information based on their specific digital fingerprints. These two technological applications are computationally complementary yet distinct. Applied to our research, distributed storage can be used to store files while their unique identifiers (*hash*) are held on a blockchain. A concrete example of distributed storage software is the "Internet Protocol Files System - IPFS"[408] . Other more or less similar, recent and complex methods enable information or even documents to be stored in the form of encryption keys. This information is distributed and hosted on different *sovereign clouds* (servers), and requires reification of the keys held by different parties in order to read the information completely. These methods of storage and IT parcelling are particularly effective in order to bring data into compliance with the European RGPD or even the *American Patriot Act*[409] which are studied further on. To ensure the regulatory compliance of an application linked to a blockchain, it is ideally advisable to host and store on the latter only *pseudo-anonymous* proofs and credentials (defined further on) that will later be useful during the identity verification process. A solution currently favored by many private and hybrid blockchains is to host sensitive data on distributed (or centralized) servers identified as trusted and supervised by certified third parties. As a reminder, a decentralized network is made up of autonomous nodes that nevertheless work together to achieve a common goal, without one or a few central nodes exercising greater (IT) power over the others[410] . Each node can make independent decisions, and data is stored locally. A distributed network is also made up of several nodes working together to achieve a common goal, i.e. with a synchronization process to guarantee the consistency of data stored in admittedly different geographical locations, but always synchronously and interconnected. Finally, while databases have complemented and replaced paper, distributed storage coupled with blockchain technology will reinforce, if not gradually replace, centralized databases. As discussed in the following sections, decentralized digital identity (IND)[411] is based on a direct, peer-to-peer relationship between people and online services. This potential industrial-scale use of

---

[407] "Hashing is the transformation of a character string into a value or key of fixed length, usually shorter, representing the original string. Hashing is used in particular to index and retrieve items from a database. This is because it's quicker to find the element based on the reduced hash key rather than the original value. This function is also used in many encryption algorithms", in *LeMagIT*, "Hachage (hashing)". Accessed June 12, 2022, at the following address. To understand this method, which uses the SHA-256 algorithm, you can enter any type of input on this site and obtain a new "*hashed"* output *of* fixed length. The slightest change to your *input data* will result in a complete change to your output data: input of the term "Right" outputs the *hash* "664a0432f64f145190913228c4d7357ed74247e93df343f935e8e83f2ba358b6"; input of the term at term "right comes out a new *hash* completely different « a6993f8f3f26eb9a2f2d232636bc47c0a0a3a819a098063e4c95127a25a460e1 ». Here, a simple capital letter demonstrates the uniqueness of each *hash* derived from an initially entered data, *see* also Appendices 3 and 6.

[408] For further information, visit www.ipfs.io

[409] See *infra,* I, Title 2, 1.5.

[410] V. Appendices 3 and 6

[411] See *infra*, II, Title 1, 1.1

distributed servers and/or blockchain technologies, would enable people to move closer to a peer-to-peer (P2P) model of social and identity interaction, similar to that which we experience in the real, physical world. In this way, no entity would control or hold identity data unless accompanied by total transparency and systematic consent for every online interaction. In this respect, a new P2P computing protocol made its appearance in early 2020: the "Nostr" protocol ("Notes and Other Stuff Transmitted by Relays")[412] . Nostr is a simple, open protocol for creating interoperable, decentralized and censorship-resistant online social media (no algorithmic targeting or information control). It's a protocol that doesn't depend on a central server, and is designed to be easily accessible via a public and private key, with the aim of creating a censorship-resistant, P2P global social network. In its most basic form, it enables Internet users to exchange signed messages via a network of relays, which are servers that any Internet user can operate. Since its launch, the bitcoin community has rapidly adopted this protocol, and various platforms have sprung up to count over 200,000 users by April 2023[413] . Nostr is therefore part of the continuity of Web 2.0, while at the same time forming a new building block for Web 3.0 and appropriately supporting digital assets such as bitcoin.

2.3.1.1.d IT and legal understanding of intelligent contracts (AEC)

Better known to the general public under its English-language appellation of "*smart contract*" and generally subject to literal translation into French by the term "*contrat intelligent*", this new application underlying blockchain technology became popular during its IT emergence in 2015[414] , its concept having first appeared earlier in the mid-1990s[415] . Since January 15, 2021, smart contracts have been renamed as "*automate exécuteur de clauses - AEC*" by the aforementioned Commission d'enrichissement de la langue française[416] . This recent translation aims to promote the use of the French language by applying a new translation for an older English concept and term. But this translation is complex and unintuitive, which is why this study uses the term "*intelligent contract*"[417] , or the abbreviation AEC suggested by the Commission d'enrichissement de la langue française.

[412] For more information on this protocol, *see* the project's Github address or the following address.
[413] For more information and real-time statistics, visit the following link. To view a social network profile using Nostr, visit the following link.
[414] When the Ethereum blockchain for the first time enables a new type of native transaction on its blockchain, allowing the deployment and execution of smart contracts ("*Contract deployment transactions"*).
[415] The concept of the "*smart contract"* has been around for decades, and was pioneered by cryptographer and computer scientist Nick Szabo in the mid-1990s. According to him, a smart contract is a computerized transaction protocol that executes the terms of a contract. Its objectives are to satisfy the contracting parties according to common, predefined contractual conditions.
[416] Commission d'enrichissement de la langue française, January 2021, *v*. Vocabulaire des actifs numériques. Text 108-B.
[417] Even if the use of this term is misleading, as a *smart contract* is in reality neither *intelligent* in the sense of artificial intelligence, nor necessarily a contract in law in the sense of common law. See also "Les smart contracts, étude de droit des contrats à l'aune de la blockchain", LEVENEUR Claire, Thèse Université Paris-Panthéon-Assas, December 2, 2022.

French. On a semantic level, the term "*smart*" is misleading, as it seems to refer to relative independence, or even autonomy, in terms of decision-making, which is not the case, as an AEC currently requires human supervision via the involvement of a developer. Through these smart contracts, it seems that blockchain technology is becoming all the more the bearer of (cryptographic and social) norms, conceived by its community, but whose legality is being questioned by some legal experts. With blockchain technology, the entire contractual value chain would gradually be shaped by code. Often considered as unidentified legal objects, AECs are an integral part of this hypothesis. To put this concept into context, we need to understand that, with the birth of other blockchain technologies (i.e., after Bitcoin), new functionalities and innovative applications have emerged[418] , sometimes with increasing adoption in IT, economic and legal ecosystems[419] . The founding idea behind these automated programs is to free ourselves from large digital platforms
2.0 and, more generally, of all trusted third parties when carrying out socio-numerical exchanges with different functions (financial, contractual, political)[420] . In February 2022, the European Commission proposed a first legal definition of a smart contract in its "Data Law" proposal (*see* following pages): a "*computer program stored in an electronic registry system, with the result of the program's execution recorded in the electronic registry*"[421] .

In computer language, a smart contract can be defined as an autonomous, distributed computer program, using blockchain technology and varying in functionality and complexity. The latter is necessarily created and programmed by a developer, directly within a blockchain and thanks to a dedicated interface[422] , accessible to all within the framework of open blockchains. Its main idea is to determine interactions and relationships between parties (rights and obligations) thanks to a computer program that will automatically administer them as soon as it is published on a blockchain (in a transaction)[423] . While conceptually, a contract is merely a theoretical framework that delimits the conditions of a given transaction between parties, a smart contract carries the principles of dematerialization, autonomy and predictability, i.e. trust 3.0 by assumed design. This means it can help facilitate, verify and enforce the performance of a virtually and legally formed contract. The use of smart contracts

[418] *Op. cit,* "Blockchain and the Law," Harvard University Press. Location 875 of 7004.
[419] SCHREPEL Thibault, "Smart Contracts and the Digital Single Market Through the Lens of a 'Law + Technology' Approach", in *European commission*. 2021. Available at
[420] According to a study by PWC in 2022, "37% of blockchain players use Ethereum worldwide", "Blockchain & crypto: how do businesses benefit?", available at the following address. This study should be put in perspective with Appendix 6.
[421] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules for fairness in access to and use of data ("Data Regulation") (2022/0047 (COD), *v.* Art. 2 recital (16), p.47. This text is available online. The *Data Governance Act, meanwhile, was* passed in May 2022 and will come into force in September 2023.
[422] Writing such a computer program requires in-depth knowledge of traditional programming or of a specific blockchain protocol.
[423] V. Appendix 3

could thus help make contractual transactions safer, more transparent and more efficient. However, not all blockchains are capable of supporting the execution of smart contracts. Only those with an appropriate protocol can store and execute such programs[424] . Once these programs have been written and compiled to optimize their execution on a blockchain (limited storage and bandwidth), they are automatically executed according to the conditions and computational rules that compose them. These lines of code can thus comply with legal rules, provided the developer has specific guidelines on the subject or legal expertise. The main characteristics of a smart contract include its supposed immutability, thanks to its underlying technology: the blockchain[425] . Its autonomy of operation and interaction is also a source of time savings, depending on the multiple parameters that can be defined within it. In theory, a smart contract can be implemented in all kinds of services that involve computer programs, while at the same time being able to exchange value. With an AEC, the transparency and efficiency of an exchange can be controlled by digital and cryptographic mechanisms (a value interaction being possible here thanks to a valuation and counterparty in crypto-assets).

Once written and recorded on a generally open blockchain, a smart contract thus becomes public (the code of this program is readable and verifiable on this blockchain)[426] . This means that anyone can freely consult their transactions (transfers of crypto-assets, tokenization of voting rights, anchoring of hyperlinks or documents[427]) carried out automatically and almost instantaneously on the blockchain on which the AEC is based. Automation is certain, speed of execution is assumed to be latent, and deployment and transaction costs are in principle reduced compared with the intervention of traditional trusted third parties (notaries, lawyers, for example). By modifying conventional financial and contractual habits, it seems that AECs could represent a new tool at the service of contractual procedures and common contract law. IT security and automation can bring greater legal security and efficiency to contractual relations. For example, in the event of non-performance of a contractual obligation,

---

[424] For example, the Bitcoin blockchain does not currently allow smart contracts as complex as those existing on the Ethereum blockchain, due to their differences in protocols, programming language and long-term conceptual vision. Bitcoin favors a simple, robust network, which nevertheless allows the deployment of certain basic, autonomous programs akin to smart contracts: *Discreet Log Contracts (DLCs*). These enable parties to place bets using the Bitcoin blockchain and the Bitcoin asset (BTC). To establish a contract, two parties sequester funds in a shared or escrow address (multisignature). These funds can only be spent when a trusted third party (called an oracle) publishes and sends the requested information at a specific point in time. With this practical example, we can see that the Bitcoin blockchain will probably host the equivalent of AEC on its infrastructure in the medium term, given the multiple protocols currently under development, such as *Lightning, Taproot and Taro*, which are discussed in Appendix 3 (Focus 3), and other protocols that do not yet exist. See also Appendix 3.

[425] LEVENEUR Claire, "Les smart contracts, étude de droit des contrats à l'aune de la blockchain", December 2, 2022, in. *Theses.fr*, Université Paris-Panthéon-Assas, pp.3-5.

[426] LASSEGUE Jean, GARAPON Antoine, "Dans la blockchain, les termes encodés du contrat (qui ne sont plus des mots) font immédiatement ce qu'ils disent en exécutant leur programme", *op. cit.* in "Justice digitale", p.162.

[427] V. Appendix 3, Focus 3.

The latter is directly recorded and visible within the smart contract, which explains the cryptographic and social probative value that blockchain users attribute to FACs. The public nature of smart contracts also enhances their auditability, which is now possible digitally at any time, by interested parties as well as third parties. The lines of computer code in an AEC can thus specify both the obligations to be met by the parties involved, and the steps involved in executing their obligations in real time. In these decentralized programs, it is possible to comment on each line of code and its IT effects, a practice that should be transposed into law and encouraged to promote a better legal understanding of these programs. These features and this transparency by design promote a form of contractual fairness for the contracting parties. Already today, and a fortiori in the future, an intelligent contract will enable autonomous players to develop fully personalized, highly complex programs, with impacts that are already unprecedented for certain social interactions, notably financial[428] . While the conditions stipulated in a smart contract are automatically enforced and verifiable thanks to blockchain technology, this autonomy and freedom of design also makes it possible to program the rules and conditions necessary for the proper contractual protection of the parties. According to a report by a working group of lawyers and scientists[429] , three main forms of smart contracts can be distinguished:

(i) Intelligent natural-language contracts: these automatically execute all or part of existing contractual obligations in natural language (classic contract). It is not used to record contractual obligations, but rather to provide a digital medium for the parties to perform their respective obligations.

(ii) The hybrid smart contract: in which certain contractual obligations are recorded in natural language and others are recorded and programmed directly into the smart contract in the form of conditions and rules. Some services are already bridging the gap between the world of computer code and that of legal codes[430] .

(iii) The (im)pure intelligent contract: there is no natural language version of the agreement and its conditions, which means that contractual obligations exist only latently, since they are recorded in the code and executed by it without a natural language contract. The latter type of contract is in widespread use today, for example in the following organizations

[428] Reference is made to Decentralized Finance, which enables Internet users to benefit from variable and risky interest rates that are unprecedented compared to those offered by traditional financial institutions.
[429] The LawTech Delivery Panel & UK Jurisdiction Taskforce, 2019, "Legal statement on cryptoassets and smart contracts", accessed online 12 January 2021.
[430] The OpenLaw website allows since 2019 to write contracts in natural language and then automate them on the Ethereum blockchain from a dedicated interface, visit openlaw.io

(DAO) or for decentralized finance (Defi) mentioned below, often with the intention of evading the legislation in force.

Based on these non-exhaustive distinctions between smart contract types, it seems that the likely future of these 3.0 computer programs is, in natural language in the short term, hybrid in the medium term and (im)pure in the long term. In terms of cybersecurity, smart contracts, mainly based on the Ethereum blockchain[431] , are programs developed in new computer languages, whose programming flaws regularly make the headlines (losses and theft of crypto-asset funds)[432] . However, the technical uncertainty of smart contracts should not be confused with the theoretical robustness of public blockchains (see Appendix 7). While the hacking of an AEC means that the Ethereum blockchain ecosystem is vulnerable, this insecurity of the decentralized application should not be confused with the lesser insecurity of its main protocol, which seems more tried and tested since 2015 (see Appendix 6). In this respect, to promote and guarantee minimum IT and legal security for AECs from trusted third parties, this research argues that Law no. 2022-309 of March 3, 2022[433] for the implementation of a "*Cyber Score*"[434] should aptly include smart contracts, in the same way as online platforms or messaging systems. From a legal standpoint, because many smart contracts involve the provision of an online service between a professional and a private individual, they must comply with the legal obligations applicable to any contract concluded electronically. It should be noted that smart contracts more or less meet certain substantive and formal conditions for the formation of legally-formed contracts (between professionals and between professionals and private individuals):

[431] "A deep dive into the 5 popular smart contract development platforms and their comparison", in *CoinTelegraph*, May 19, 2022, available at, *see* also Appendix 6, Focus 2.

[432] "At the end of April 2021, major cryptocurrency thefts, hacks and frauds totaled $432 million", August 11, 2021, *v.* "Cryptocurrency Crime and Anti-Money Laundering Report", in *CipherTrace*. Available at

[433] Law n°2022-309 of March 3, 2022 for the implementation of cybersecurity certification of digital platforms intended for the general public, JORF n°0053 of 04/03/22, modifying the provisions of Article L. 111-7-3 of the French Consumer Code, which now stipulates that "Operators of online platforms (...) and persons providing non-dial-based interpersonal communication services (...) shall carry out a cybersecurity audit, the results of which shall be presented to the consumer (...) covering the security and location of the data they host, either directly or via a third party (...) The aforementioned audit shall be carried out by audit providers qualified by the Agence nationale de la sécurité des systèmes d'information".

[434] The aim of the *Cyber Score* is to combat security threats and vulnerabilities. All major public-facing digital operators, such as online platforms, video-conferencing software and messaging systems, are concerned. Startups and small businesses are not yet concerned. A decree is expected to specify the thresholds, scope and period of validity of the Cyber Score. Penalties for non-compliance could reach 375,000 euros.
for a legal entity. The aim of the Cyber Score is to reinforce the protection of players (VSEs, SMEs, the general public) by promoting secure and responsible solutions. The audit used to determine the score will be conducted by ANSSI according to several indicators (data location, security and encryption types, number of RGPD convictions, and number of software vulnerabilities updated). It will serve as an indicator of comparison between companies and become one of the valuation criteria.

Types of contracts (*no exhaustive*)	**Legal validity of an AEC as a contract validly formed**
Negotiated contract	Yes
Authentic contract	No
Solemn contract	No
Real contract	Yes or no, depending on the specific purpose of the contract
Membership contract	Yes

For the time being, AECs seem at best to qualify as quasi-contracts. For example, the provisions of articles 1125 to 1127-4 of the French Civil Code[435] concerning the formation and conclusion of electronic contracts at a distance. It is not certain that the conclusion of smart contracts systematically complies with positive law, a paradox in view of the growing daily use of crypto-asset trading platforms and financial services 3.0[436] . Thus, an amendment to the current provisions of the Civil Code concerning contract formation could make it possible to explicitly include "*clause-executing automata - AEC*". The literature has been working on this since 2018[437] , but many legal uncertainties remain, if only in terms of civil and/or criminal liability. Is it the developer or the party who has failed to comply with the conditions? Undoubtedly, and as is often the case in legal matters, this will be assessed on a case-by-case basis. For the sake of completeness, the European digital strategy should mention several EU texts that are essential to the legal framework for data impacting on smart contracts. Data Governance

[435] Articles 1112 to 1127-4 of the Civil Code, in the version in force since October 1er 2016, Subsection 4: provisions specific to contracts concluded electronically of Section 1: conclusion of the contract.
[436] Reference is made to the aforementioned concept of "Decentralized Finance" ("DeFi"), which brings together numerous pseudo-decentralized financial platforms and services (*v.* crypto-asset platform/exchanges named Uniswap) aimed at crypto-asset holders.
[437] Maître GIUSTI Jérôme, "Are 'smart contracts' contracts?", March 31, 2018, in *Metalaw*, accessed June 11, 2022, at.

Act (DGA)[438] , a European Regulation on data governance that was voted in May 2022 to come into force in September 2023, followed by a legislative proposal for a new Regulation, the "Data Act (DA)"[439] , drafted for the benefit of businesses with a consequent component on the Internet of Things (IoT/IoT), coming alongside the "Digital Markets Act - DMA" which was voted on October 19, 2022, and the "Digital Services Act - DSA" voted on October 27, 2022. Other proposed regulations are currently under discussion, such as the "e-privacy" regulation and a future "AI" regulation dedicated to artificial intelligence[440] .

The DA's draft does not specifically mention the crypto-asset industry. Some players in this industry are concerned about the consequences of its entry into force in September 2023 on smart contracts. As it stands, there is a "*presumption of compliance*" for non-financial smart contracts, dedicated to the management of data from legal entities, natural persons or machines (connected objects). Under Article 30, the vendor of a smart contract, or the person whose business involves the deployment of smart contracts for third parties under a data provision agreement, would have to carry out a "*compliance assessment*" and issue a declaration of compliance for these contracts. This person then becomes responsible for compliance with four requirements[441] . If the scope is ever extended to include (crypto)financial smart contracts, then the latter will not be able to comply with such requirements. Such an extension would have similar consequences to the MiCA Regulation's attempt to ban *proof of work,* which was rejected *in extremis,* as discussed below[442] . In practice, this *presumption of compliance* will be granted to non-financial smart contracts (management of machine-derived data), but does not apply to the massively used (crypto)financial smart contracts currently in use. These rules aim to create a form of smart contract standardization with a new class of centralized, controlled and hybrid AECs, where the immutability of transactions is discarded. The real impact of these rules remains to be determined through future dedicated implementing acts. This provision thus seems to echo the *presumption of reliability that* is also granted under certain conditions to "*electronic registers*" (blockchains)[443] within the meaning of the eIDAS-2 Regulation.

---

[438] Regulation (EU) 2022/868 of the European Parliament and of the Council of May 30, 2022 on European data governance (Governance Regulation) and amending Regulation (EU) 2019/1724 on data governance, v. the White Paper "Data governance: organization and strategy to adopt in 2023", in *DataValue consulting*, downloadable from *dataconsulting.com*

[439] Proposal (EC) for a Regulation of the European Parliament and of the Council establishing harmonized rules for fairness in access to and use of data (Data Regulation), 2022/0047(COD), February 23, 2022, *v.* available at

[440] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (artificial intelligence legislation), COM/2021/206, available online.

[441] V. Art. 30: "(...) robustness, interruption capability, access control and audibility (...)".

[442] V*, infra*, I, Title 2, 2.5

[443] A second semantic blur in the Data Act concerns the reference to the term "*electronic register*" (art. 2, 16 & 17), which refers to "article 3 point 53" of the eIDAS Regulation. However, this reference does not define the term (which does not exist in eIDAS). By extension, it is likely that the term "electronic register" in the Data Act refers rather to the "electronic register" in the eIDAS Regulation.
The term "electronic time-stamping" is defined in point 33 (not "53" as in the Data Act). This can be a source of confusion, as the Data Act mentions the term electronic registry in the definition of a smart contract, whereas it

Whether it's an attempt at technological reappropriation for some, or technological dressing-up for others, it's still early to tell, and only the acts of execution mentioned will enable us to determine[444] .

As a result, smart contracts are still mainly used in 2023 in the context of (crypto)financial relationships and contracts, i.e. relating to crypto-assets. However, as its concept and underlying blockchain technology become more widely adopted, other use cases will emerge, notably relating to digital identity attributes. Note that when several smart contracts are linked to each other (one to manage financial transactions, another managing voting rights, etc.), they form the concept of "*decentralized autonomous organization - DAO*"[445] which is explored further below, so that their beneficiaries and users can replicate the operation of a legal entity, but in a transparent, accessible and dematerialized way[446] . Finally, smart contracts should not be considered in isolation, as their applicative potential remains partially unknown, as demonstrated by their re-appropriation by non-fungible tokens (NFTs)[447] between 2020 and 2022. We argue that in the near future AECs will be a pillar of self-sovereign digital identity management, studied in title two of this study. A majority of private blockchains and consortia are compatible with the creation and management of AECs, as they are derived from the public version of the Ethereum blockchain that saw the birth of this concept of autonomous, decentralized programs. While smart contracts partially defy the rules of law through computer code, but also by diminishing the role of the judge in adjudicating a dispute, the conditions of formation and execution of AECs are legally covered by ordinary contract law, as more and more legal experts seem to be gradually reminding us[448] .

Strictly speaking, this is a reference to the notion of electronic time stamping within eIDAS, and not, as is possible, a reference to the notion of "distributed registry" as provided for in the MiCA Regulation (*see* art. 3, 1). This might seem more coherent, as smart contracts can only exist electronically on a "*distributed register*" (MiCA) and not on an "electronic timestamp" in the sense of eIDAS and as currently drafted in the Data Act. It seems that this confusion leads to a form of semantic misunderstanding with regard to computer science, as well as the need in law to replace the term "electronic register/timestamp" by "distributed register".

[444] See Chap. XI "Final provisions", available at the following address

[445] See I, Title 1, 2.3.1.1.f *below.*

[446] *Op*., *cit.* "(...) the mini-communities created by blockchain claim to institutionalize themselves thanks to the technique", in "Digital justice", p.152.

[447] The term "JNF" has made its debut in the 2023 edition of Larousse, with the following definition: "A non-reproducible and unforgeable digital file representing a unique asset, virtual or physical object (work of art, tweet, piece of music, etc.), which is listed in a blockchain and to which is associated a digital certificate of authenticity and ownership.". While this definition is open to improvement, particularly with regard to the notion of uniqueness of the assets to which a JNF belongs (often neither unique nor rare), it remains particularly close to the IT and practical reality of the uses made of these digital objects in 2022. *see* also *infra*, I, Title 1, 2.3.1.1.f

[448] See I, Title 2, 2.7.1 *below.*

2.3.1.1.e Ricardian contracts for enhanced contractualization 3.0

Computer programmer Ian Grigg observed that "*while some people see problems as having contracts to solve them, our problems are contracts*". This observation led him to create the concept of "Ricardian contracts"[449] . In 1995, he invented this new concept and initially called it the "Ian Grigg Ricardian contract". The name was chosen as a tribute to David Ricardo, a famous English liberal economist and major contributor to international trade theory. In 2016, Oliver Hart and Bengt Holmström were awarded the Nobel Prize in Economics for their work on the incompleteness of contracts and its consequences for the economy. However, Ian Grigg found a solution to the complexity of contracts long before the Nobel Prize was awarded. Contracts are often imperfect and incomplete due to unforeseen risks that may arise before or after they are signed. Ian Grigg proposed that the programming and automatic execution of certain clauses could considerably reduce the problem of complexity and efficiency associated with traditional contracts. Unlike the latter, automatic contract enforcement could improve clarity and efficiency while saving valuable time for the parties involved. The invention of the "Ricardian contract" dates back to 1995, but the term was first used in an academic publication in 1998[450] . It was not until 2004 that a publication specifically dedicated to the subject detailed the origin of the problem and the solution proposed by Ian Grigg[451] . In addition to creating the concept of the Ricardian contract, Ian Grigg is also known in the blockchain world for his work on cryptocurrencies in the 2000s, notably with his startup DigiCash[452] . In essence, a Ricardian contract is an innovative concept that links a paper contract to its programmed digital version in order to make the execution of certain of its clauses automatic. It complements the hybrid smart contract mentioned above. This contract is legally binding and can be read by computers as well as by legal professionals. It consists of a document completed and signed by the parties, which exists in two forms: one as code readable only by computers, and the other as human-readable text. The Ricardian contract is presented in the form of a text with several parameters to be filled in, which are self-executing once validated. This clever approach has earned it the name "Wise contract", as it allows the contract to be read, understood and executed at the same time.

The Ricardian contract can be defined as a contract model accessible to all, which makes it possible to generate a document (i) readable by humans, (ii) executable by a computer, (iii) digitally signed[453] ,

[449] KRYPTOSPHERE®, "Ricardian contracts, the future of smart contracts?" in *Cryptoast*, online, published September 5, 2020.
[450] GRIGG Ian, "Financial Cryptography in 7 Layers", 1998-2000, available at
[451] *Op. cit.* "The Ricardian Contract", accessed July 29, 2021.
[452] See I, Title 2, 1.4.1 *below.*
[453] Once the parameters have been met, the contract is signed using a *private key* or other similar protocol (such as PGP). This signature constitutes proof of a party's intention.

(iv) containing the private keys of the parties or computer servers involved, and (v) being able to possess a unique identifier[454] . This invention aims to overcome the barrier that separates the machine world from the human world. Traditionally, contracts exist in paper or digital form, but are read exclusively by humans. Computer programs, on the other hand, can only be executed by computers. Their separation creates a gap where complexity can nestle. The Ricardian contract creates an unprecedented bridge between man and machine to bridge this gap. In the history of computer science, the Ricardian contract can be seen as a precursor to the intelligent contract. Indeed, as early as the 2000s, Ian Grigg had already understood the importance of automating the execution of certain clauses in digital contracts, which is now a key feature of smart contracts. Thus, in creating the Ricardian contract, he responded to this problem by creating a single document that could be both legally valid and transparently and incorruptibly enforceable on a public, private or hybrid blockchain. Initially, Ian Grigg had designed the Ricardian contract for the financial sector, and more specifically for the issuance of complex financial products. However, as of 2019[455] , the online sales platform OpenBazaar has adopted this new form of contract, testifying to the diversity of possible use cases for this ancient yet still relevant IT and contractual system. In principle, a Ricardian contract needs to be stored with one of the parties or a third party, to be digitally preserved and then executed via an interface. In this respect, the blockchain or P2P servers mentioned above offer their complementarity, interest and relevance. The contract can then be stored and executed on a distributed or decentralized[456] electronic registry, with the various advantages that this may imply (compliance, security, transparency, data integrity). As we have explained, a Ricardian contract is first and foremost legally valid, and secondly, self-executing. Where a smart contract can only be a means of executing a contract on a blockchain (the legally formed contract being a separate document), the Ricardian contract is both a contract and a means of execution on a blockchain and/or centralized server. A smart contract cannot predict the outcome of many situations that may arise in a contract, as contracts are imperfect by nature. Indeed, a smart contract can foresee the cessation of its execution, but not the definitive outcome of a situation. In the event of failure to automate some of its clauses, a Ricardian contract by design provides for an outcome legally approved by the parties, such as referral to an arbitrator or judge. In this respect, it is possible to imagine Ricardian AECs or contracts

[454] This is simply the *hash of* the contract once it has been digitally signed by the parties. A *hash* is a sequence of numbers and letters of a given length resulting from the passage of a file through a hash function. Whatever the format and size of the file, the *hash* will always be of the same length, but will never be the same. A simple change of a single letter in a text of thousands of pages will radically alter the hash, enabling the integrity of the contract to be attested.

[455] LOPAMUDRA Mandal, "Ricardian contract: Bridging the Gap Between Smart Contracts and Traditional Contracts", Master Thesis, International Business Law, June 2019, p.10, available online at.

[456] Here, an important distinction needs to be made between a *distributed registry*, which allows data to be stored, and a *decentralized registry (blockchain),* which only allows proofs of data to be stored and not the entirety of the data (for computational reasons such as prohibitive storage costs when carried out on a decentralized blockchain).

have arbitration clauses providing for decentralized dispute resolution (v.
"Kleros"). In short, Ricardian contracts offer greater security than paper contracts, thanks to their cryptographic signature which is difficult to usurp and counterfeit. They also make it possible to automate all or part of the contract, which can save considerable time and human and financial costs. However, according to Ian Grigg, it is not always beneficial to automate all the clauses of a contract, as some are too complex and unpredictable. Consequently, it is likely that only contracts of low complexity and repetitiveness will be fully automated, while others will be hybrid contracts that aim to satisfy the legal requirements of the parties. What's more, according to Ian Grigg, the professionals concerned may not need or be interested in digital contracts, whether "smart" or "intelligent".
"The role of lawyers cannot be totally replaced by these contracts.

2.3.1.1.f Decentralized autonomous organizations (DAOs)

As doctor and author Primavera De Filippi explained back in 2016: "*if blockchains improve in terms of speed, performance, functionality and accessibility, the technology could, in the longer term, begin to structure organizations that compete with traditional corporations and other legal entities* (...)". In 2022, a Decentralized Autonomous Organization *(DAO)* can be simply defined as an online community structured on a blockchain protocol[457] . This is a new type of organization that appeared in 2016 and operates using smart contracts on a blockchain. This means that it is a digital entity that operates automatically, with or without human intervention, according to a set of rules encoded in FACs. These rules determine how the organization is managed, how decisions are made and how it interacts with other entities on the blockchain. The promise of DAOs is to help transform the governance of the Internet, and more specifically of its online services, notably by proposing to co-construct them by involving their users in the chain of decision-making, i.e. in their governance. In other words, a DAO is a digital organization that reproduces on a blockchain the actions and interactions specific to any organization, such as voting rights, financial transfers and messaging services. Consequently, a DAO is a virtual entity (generally without structure or legal status) in which all interactions are carried out by means of smart contracts on a blockchain. There are as many DAOs as there are virtual environments and contexts, available to crypto-asset holders who wish to found or join a DAO. The autonomous nature o f a DAO means that some of its

[457] "It [DAO] allows groups to be founded by contract, but without an initial political contract or statutes (...)", *op. cit.* "Digital justice", p.148.

interactions can be programmed and automated according to the rules of their founders and communities. Its decentralized nature implies that no intermediary can censor it or prevent it from functioning properly[458] , an observation that is regularly called into question in practice due to the intrinsic need for trusted third parties at the heart of the creation of these entities, which are in reality profoundly social and therefore hierarchical and centralized. As in the case of smart contracts, a case-by-case approach to the question of whether a DAO is decentralized or not seems appropriate, as it implies a very different legal qualification depending on the situation and jurisdiction. In principle, all DAOs are decentralized, which means that they are not controlled by a single person or group, but rather by all the members who participate in their operation (users, developers and contractors). This enables them to operate transparently and democratically (with all members having an equal say in how the organization is run, for example). On a semantic level, the term "autonomous″ in the DAO acronym is as misleading as the term "intelligent" attributed to AECs. Rather, it refers to an automated system, not a technically independent, autonomous one. A similar observation can be made with regard to the use of the term "decentralized", as a CAD is often controlled by a more or less large group of players, such as individuals or companies (see below).

It's important to note that the power of governance within these digital communities is shared between members through smart contracts that aim to create a free and independent online community. In theory, every decision and rule of a decentralized digital community is subject to the collective appreciation of its other members (voting rights, crypto-asset exchanges, private messaging, peer review process, etc.). Although DAOs have existed on Ethereum since 2016, these early computing and social experiments represented full-scale scientific projects (experiments), rather than marketable products accessible to the general public. However, since December 2020, DAOs have become a practical necessity within the crypto-economy and a concern for some legal experts. The first quasi-industrial vector in the deployment of this technological concept has been put into practice by "*Decentralized Finance - DeFi*" protocols, which in order to develop (sometimes to evade financial regulations)[459] , have handed over more or less control of their protocol(s) into the hands of

[458] *Ibid*: "The decentralized autonomous organizations [DAOs] are no longer localized on a given server, and are nobody's property.

[459] However, in this nebula of *decentralized finance*, we consider that the legislator can always find an entity or official to turn to and therefore who can be regulated. In this regard, the European Commission issued a 15-month call for projects on October 5, 2022 - to the tune of 250 million euros - to provide a framework for this new market segment of blockchain technology. In particular, the aim is to "develop, deploy and test a technological solution for the embedded supervision of decentralized finance (DeFi) activity. The project will seek to take advantage of the open nature of transaction data on the Ethereum blockchain, which is the largest settlement platform for DeFi protocols. It will focus primarily on the automated collection of monitoring data directly from the blockchain to test technological capabilities for monitoring DeFi activity in real time.", free translation from English, in *TED - Tenders Electronic Daily*. Retrieved October 19, 2022, from

their community(ies) and users. This type of operation, which is very popular between 2020 and 2022, works in such a way that these users vote thanks to utility and governance tokens that they acquire directly on their personal addresses, which are themselves registered and linked to these DAOs, so as to influence the development of these projects with their sometimes dubious promises. Extending the point, the creation of a DAO on a blockchain enables an entity to benefit from the same advantages inherent in blockchain technology, such as the decentralization of interactions, security, speed, transparency and immutability[460] . On the social and political front, many in the crypto-economy suggest that a DAO comes close to a pure democratic system, similar to those of ancient Greece. If DAOs do indeed enable the creation of a new, decentralized multitude of digital communities, this assertion seems utopian, if only in view of (i) the formation of a DAO and (ii) its effects on its users.

(i) When a DAO is set up, its capital of digital tokens is first created and then distributed to its users. This issuance of tokens is thus subject to initial centralization by a few players or entities, who in the majority of cases represent the DAO's actual and majority beneficiaries. In principle, the more tokens a person owns, the more decision-making power he or she has (in the same way as holding shares in a commercial company, for example). As capital ownership is at the heart of this centralized governance system, it should not be confused with its blockchain protocol (which is itself decentralized[461]), as is often the case outside this ecosystem.

(ii) DAO governance systems are therefore numerous, and all computerized and socially centralized. Users with a low level of participation in governance and fewer tokens may suffer unintended consequences, including the risk of manipulation by users with larger numbers of tokens. This could result in significant financial losses for small holders. What's more, in the event of fraud, theft or error, responsibilities are complex.

In addition, a new report published by the European Commission proposes four measures to frame this ecosystem: (i) regulate legal entities (macro-prudential provisions, etc.), (ii) introduce a voluntary framework for DeFi supervision, (iii) create a public observatory that issues opinions based on data from public blockchains ("*integrated supervision*") and finally (iv) build an approach for the supervision/regulation of *oracles* (an oracle is a trusted third party used to transfer trusted information to a blockchain). FISMA: Directorate- General for Financial Stability, Financial Services and Capital Markets Union. 2022. "Decentralized finance: information frictions and public policies: approaching the regulation and supervision of decentralized finance". Retrieved October 24, 2022, from

[460] By way of illustration, here's a DAO based on the Ethereum blockchain to better understand the previous explanations. This DAO was used for experimental purposes between 2019 and 2021. By browsing its interface, we can see that it allows users to vote, deposit or withdraw crypto-assets (ethers) or exchange messages directly via the Ethereum blockchain.

[461] V. Appendix 7.

to define and those responsible to identify due to pseudo-anonymity[462] studied under the next heading of this study, as demonstrated by legal expert Primavera De Filippi: "*any action against promoters or token holders may deter interest but will not necessarily put an end to these organizations.* (...) *Indeed, even with a court order, traditional enforcement mechanisms may struggle to reach assets controlled by a decentralized organization*"[463] . Furthermore, the fact that each DAO operates in a unique way and that its digital tokens can be classified in one or more of the categories of one or more (crypto)taxonomies and jurisdictions, depending on their nature, purpose or characteristics, complicates any legal qualification. To date, the majority of DAOs are not legally registered, except in the state of Wyoming, which was the first state to create an ad hoc legal regime dedicated to these decentralized organizations[464] . Finally, as Ethereum co-founder Vitalik Buterin partially admitted in 2022: "*realistically, we probably only need a small number of DAOs that look more like constructs from political science rather than DAOs operating in a way similar to corporate governance. But these are the most important*"[465] .

Consequently, in order to meet some of these digital and legal challenges, a recent report by the French National Assembly[466] proposes recognizing DAOs as a legal entity with legal personality. The aim of this proposal, which this research supports, is to adopt an *ad hoc* legal framework for these digital entities, notably by requiring them (i) to comply with the regulatory obligations in force in France (registration as a PSAN[467]), (ii) to identify the identity of digital token holders and beneficiaries, and (iii) to put in place safeguards

[462] See I, Title 2, 1.4.1 *below*.
[463] *Op. cit,* De FILIPPI Primavera. "Blockchain and the Law," location 2835 of 7004.
[464] The U.S. state of *Wyoming* has legally recognized a DAO as a limited liability company, with special provisions allowing the company to be directed or managed algorithmically (in whole or in part) by *smart contracts*. This bill creates a supplement to the Wyoming Limited Liability Company Act to provide a law controlling the creation and management of a DAO. The provisions of the Limited Liability Company Act apply to a DAO unless specifically modified by the supplement. This bill establishes basic requirements for member-managed or algorithm-managed DAOs and provides definitions and regulations for DAO formation, articles of organization, operating agreements, smart contracts, management, standards of conduct, member interests, voting rights, member withdrawal and dissolution. Sixty-sixth legislature of the state of Wyoming, 2021, "SF0038 - Decentralized autonomous organizations", in www.wyoleg.gov. accessed June 12, 2022, at.
[465] BUTERIN Vitalik, "DAOs are not corporations: where decentralization in autonomous organizations matters", 2022, Retrieved September 20, 2022, from
[466] "Proposal 22: (i) Allow DAOs to obtain legal personality in order to recognize their legal existence and give them the power to enter into contractual relationships, unlike other legal entities. (ii) Develop a regulatory framework to take into account their governance, ensure their financial stability, in particular to protect their members and guarantee their IT security", *op. cit*, "Monnaies, banques et finance: vers une nouvelle ère crypto: un enjeu de souveraineté et de compétitivité économique, financière et monétaire", Rapport de l'Assemblée Nationale, reported by former Paris deputy Pierre PERSON, 2022, p.194.
[467] BOUILLET-CORDONIER Ghislaine et al, "La Finance Numérique - Aspects juridiques et fiscaux du crowdfunding et des cryptoactifs", p.146, *op. cit.* Available at

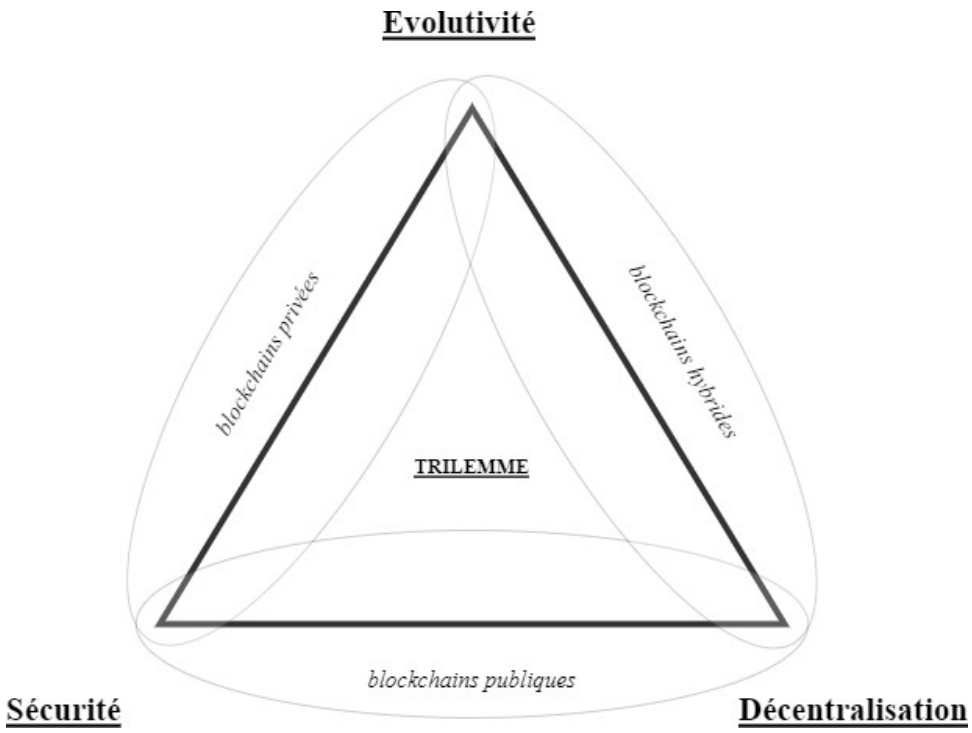
In fact, a judge could currently consider that a DAO constitutes a de facto company, or that the trust rules provided for in our positive law are fully applicable. Indeed, a judge could currently consider that a DAO de facto constitutes a company, or that the trust rules laid down in our positive law are fully applicable. It should be noted that in the UK, the *Law Commission* has been asked to undertake a 15-month study from summer 2022 to explore and describe the current treatment of DAOs, in particular to identify how they should be treated in law, and to clarify their status and facilitate their adoption[468] . In short, DAOs represent a new 3.0 tool supposedly at the service of users and online communities, following on from the evolution of Web2.0 (including blogs and social networks). Legal thinking and jurisprudence around DAOs will shape the evolution of the uses of associated crypto-assets and, more broadly, decentralized finance[469] . From a legal point of view, a grey area remains, and each national legislator seems right to let innovation express itself through these new socio-numerical vehicles of digital identity. While these 3.0 digital communities will enable the emergence of new models with a humanist vocation, yet with a capitalist operation, there is no doubt that, depending on their degree of decentralization, purpose and legal framework(s)[470] , they will benefit Internet users, both in terms of user experience and the enhanced exercise of their rights and their individual and collective obligations and responsibilities. To achieve this, DAOs must fit in with existing social and legal systems, so as to limit the phenomenon of legal arbitrage, which consists in choosing the least restrictive legislation to operate with the minimum of legal constraints.

[468] "Decentralised Autonomous Organisations (DAOs)" | Law Commission, 2022, available at

[469] In April 2023, the ACPR and the Banque de France published a report in favor of building a regulatory framework applicable to the *decentralized finance* sector, or rather "*Disintermediated Finance*" (a recent semantic distinction echoing the concept of degree of decentralization that this research studies). Measures to regulate DeFi focus on five key areas. Firstly, this report proposes the certification of blockchain infrastructures by imposing minimum standards of protection and security. Secondly, the control of intermediaries who facilitate user access to DeFi services should be strengthened, according to the report. Thirdly, an objective assessment of users' financial skills and risk appetite should be imposed. Although these measures seem beneficial for Internet users, the implementation of such proposals will inevitably reinforce a centralization of these 3.0 solutions, for example subject to mandatory certification concerning the smart contracts on which they are based. If these proposals are only theoretical for the moment, as they are accompanied by an essential survey of the players in these ecosystems, there is no doubt that the law will once again risk introducing extremely restrictive legal rules for these protocols, ecosystems and users who are simply looking for more freedom, pseudo-anonymity and online financial alternatives. v. ACPR, Banque de France. "Finance 'décentralisée' ou 'désintermédiée' : quelle réponse réglementaire?", 2023, available at

[470] "It will be a question of protecting citizens while keeping in mind the imperative need to support innovation and competitiveness in a decentralized approach", *op. cit.* National Assembly report, p. 193.

2.3.2 The incompatibility triangle of blockchain technologies

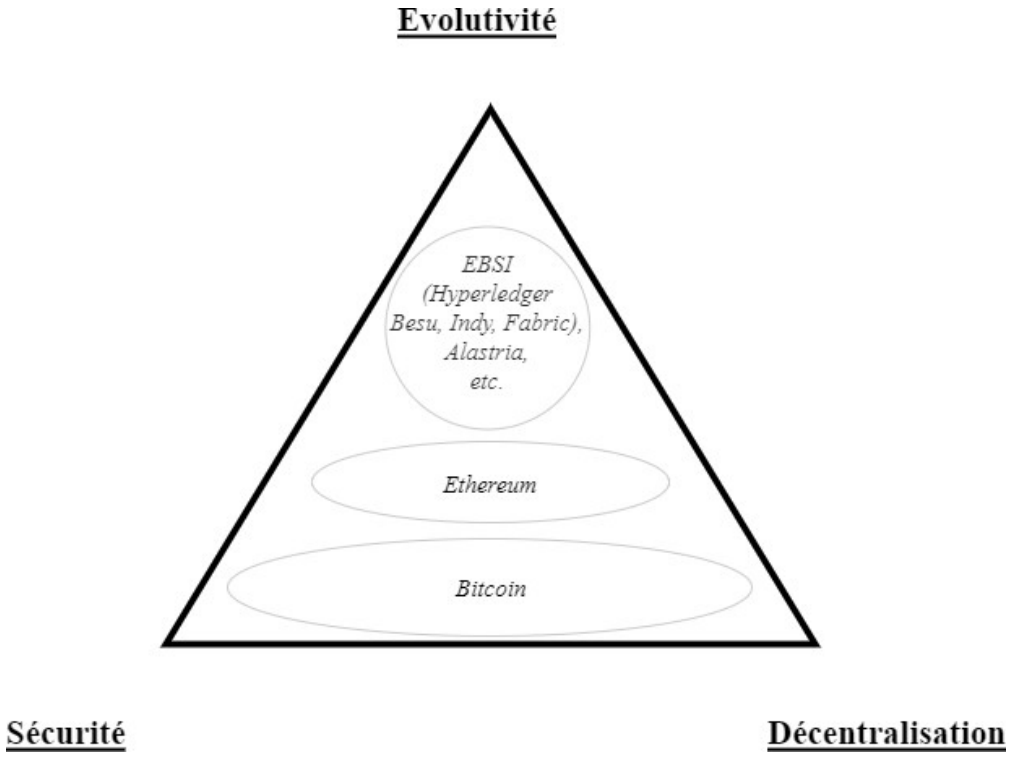


The diagram presented above illustrates a recent and renowned computer theory in the field of blockchain technology, first presented in 2017 by Vitalik Buterin. The law of

The "incompatibility trilemma" applies to any blockchain infrastructure, and states that it cannot simultaneously reconcile three aspects: (i) IT scalability, i.e. the ability to 'scale up' and evolve the infrastructure, (ii) IT security, and (iii) IT decentralization. In the diagram shown, security and decentralization are the two fundamental pillars of blockchain technology, while scalability represents the major challenge. So, how can we achieve a sufficient number of computers to ensure the immutability of the transaction register, while guaranteeing fast transaction processing on the network? In other words, this computing trilemma means that a blockchain and its ecosystem can ideally have only two possible technical choices or situations at any one time[471] . Indeed, as the second version of this diagram below demonstrates, a blockchain can only achieve or strive towards two of decentralization, scalability or security (only one side of the illustrated triangle can be achieved, and necessarily at the expense of the other two). With this in mind, compromises are inevitable when faced with the trilemma of achieving scalability, security and IT decentralization simultaneously. Consequently, an entity wishing to use a blockchain must

[471] (i) A blockchain that is highly secure and scalable (fast), but not very decentralized; (ii) A blockchain that is highly secure and decentralized, but slow to validate register transactions; (iii) A blockchain that is scalable and decentralized to the detriment of its security.

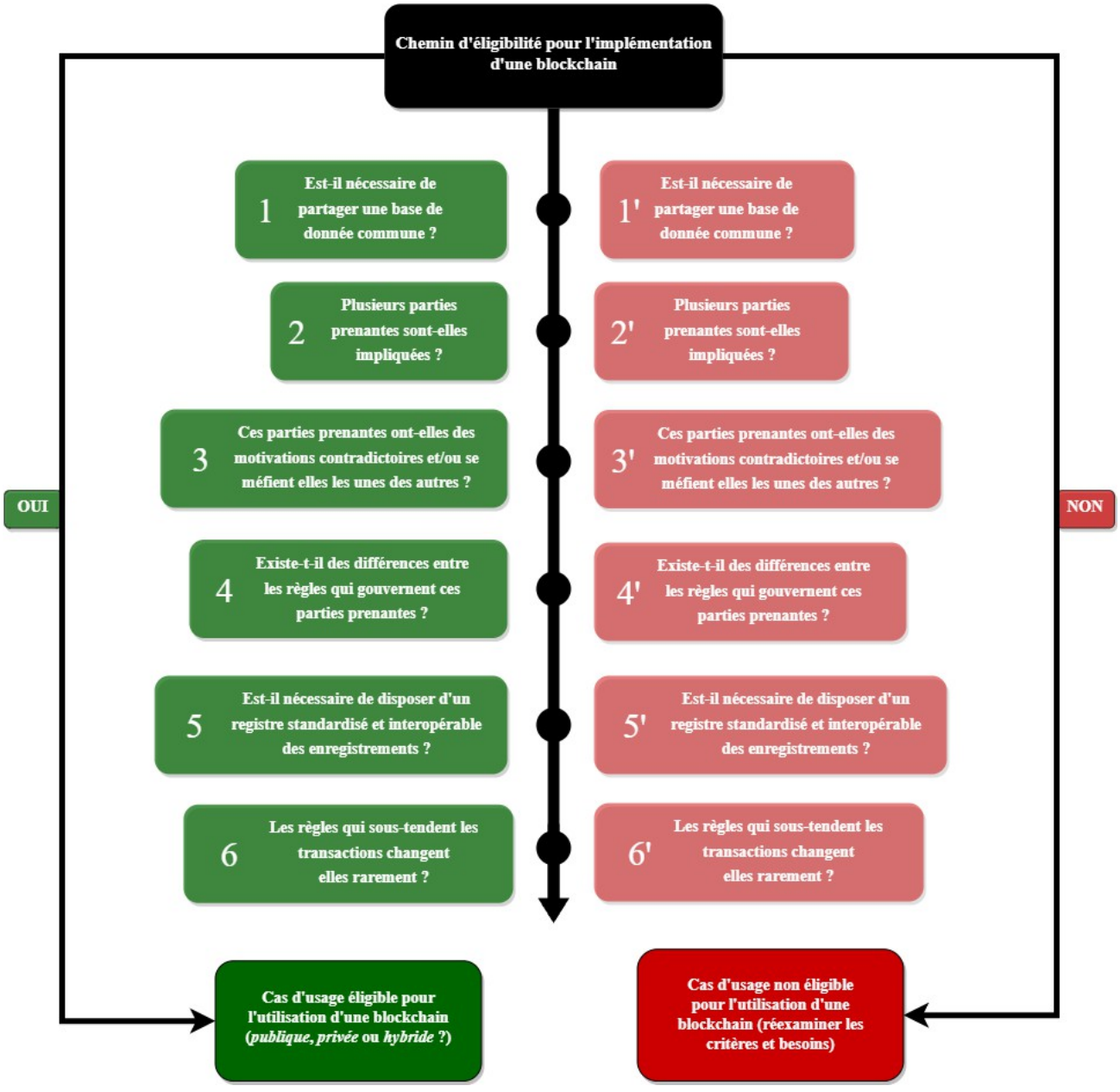
blockchains (Bitcoin, Ethereum)[472] , private blockchains (Quorum, Corda)[473] and hybrid blockchains (Hyperledger Besu, Indy, Fabric)[474] , the most (re)known to date. In this second diagram, each blockchain has a specific positioning that corresponds to its intrinsic IT parameters and functionalities, generally defined when its protocol was designed[475] . As mentioned above, even with continuous technical progress, this theoretical trilemma can never be solved by a blockchain for hardware and IT reasons. Finally, it's worth pointing out that on this diagram, the Bitcoin blockchain possesses a high degree of decentralization and security, i.e. computational resilience (*see* Appendix 3).



[472] Note that while Ethereum is a public blockchain, its computational decentralization is currently lower than that of Bitcoin, which means that its positioning on the diagram would be above and further to the left than that of the Bitcoin blockchain. While achieving *pure* or *total decentralization* is not an end in itself, it does protect the protocol and all its previous transactions from any attempt at tampering.
[473] These two projects allow companies to create their own *private blockchains*, cf. Quorum and Corda websites.
[474] This project enables the creation of *hybrid blockchains using open source* protocol suites (including other public blockchains such as Ethereum).
[475] Number of nodes, consensus mechanism (*see* Appendices 3 and 6), validation time between blocks, etc.

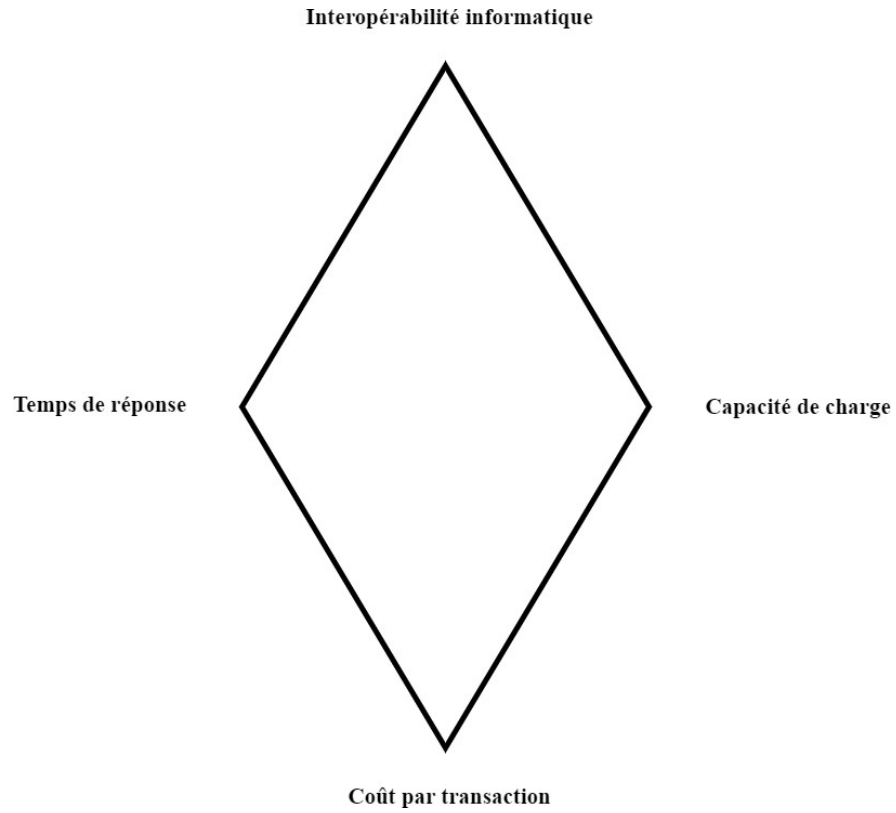
2.3.3 Eligibility path and diamond-shaped business model for blockchain technologies

It is essential for an organization to determine whether or not the use of a (semi)decentralized registry is necessary to meet the needs of its market and products. To help in this reflection, a simplified and non-exhaustive questioning process referred to as the "blockchain eligibility path" is proposed to determine whether the use of one of these technological variants is relevant for an organization.



Following on from the incompatibility triangle outlined in the previous paragraph, these few theoretical investigations propose extending this same concept to the various possible business models for a blockchain infrastructure, depending on a company's point of view and its needs in this area. Indeed, it seems possible to draw inspiration from the incompatibility triangle to propose a new "

diamond business model", which allows new concepts to be included with regard to the key success factors (KSFs)[476] that a blockchain infrastructure must meet for an industrial company to implement and use it. This theoretical model enables organizations, and especially businesses, to identify their recurring needs for numerous online services, and to observe how different blockchains can position themselves at the center of this schema.



The first, upper end of this diamond refers to "interoperability", i.e. the ability of a blockchain to communicate electronically with one or more other computer systems.
2.0 and/or 3.0 (thanks to common or equivalent technical standards). The second, opposite end ("*cost per transaction*") represents the resources required to operate and validate each transaction in the blockchain infrastructure in place (this cost varies according to the type of blockchain and its underlying parameters). The third end on the left designates
This is the "*response time*" that is computationally possible between each transaction following a request to obtain information registered on the said blockchain. As a reminder, this response time can vary from a few milliseconds for a centralized server, to several minutes for a public blockchain.

[476] VERSTRAETE Thierry, "Les facteurs clés de succès sont les éléments ou les variables déterminantes qui contribuent à la réussite d'un projet, d'une entreprise ou d'une activité", "Faut-il toujours appeler les facteurs clés de succès: facteurs clés de succès?", available at, p. 2, accessed May 18, 2021.

such as Bitcoin[477] . Finally, the last point on the right of the diamond ("*load capacity*") refers to a blockchain's ability to respond to a sharp increase in the demand for transactions in a limited timeframe (some blockchains thus set up so-called "*second computing layer*" systems[478] dedicated). It should be noted that these IT systems interconnected to a blockchain sometimes improve the legal compliance of the blockchains to which they are attached[479] .

Looking at the above eligibility path, it appears that any player wishing to use or interact with a blockchain needs to answer a number of essential questions. First of all, (i) they need to understand and identify which type of blockchain and governance are technically relevant (public, private or hybrid blockchain) and (ii) according to which use case and sector. Then (iii), a legal impact study[480] is systematically recommended to identify which laws are applicable or likely to be applicable to the said 3.0 technology/application. Depending on the legislation (iv), minimum and mandatory requirements under the applicable law (v) should be included right from the start of infrastructure or application development. Continuing on from the previous ideas and sections, it makes sense to present in a table four possible scenarios as to the conditions and probabilities of adoption for each type of blockchain:

[477] Between each block of transactions, a validation time of around 10 minutes is imposed on average, a delay that is unique to Bitcoin, reinforcing its computer security while conferring a high degree of predictability (its protocol is nicknamed the "Timechain").
[478] V. Appendix 3, Focus 4. Second-layer systems can be attached directly ("Layer 2"), or indirectly ("Sidechain"), to the main blockchain and protocol, with computing modalities that can vary in complexity and similarity. In short, a *Layer 2 relies* on the security of an existing blockchain network, while a *Sidechain* relies on its own IT security model.
[479] "Information present on a side chain [Layer 2] can be easily deleted, which also makes it possible to organize a right to oblivion not authorized by the initial logic of the blockchain.", *op. cit*. BOUSQUET Marc, "Tout savoir sur le Bitcoin et les cryptomonnaies", in *Dossiers Science Hors-Série*, édition du Sens, ISSN: 2802-1843, November 2022, p.39.
[480] Such an analysis can help answer a variety of questions, including: how can we ensure legal and regulatory compliance for blockchain? What data will be captured and exchanged? Who will have access to this information? What levels of data confidentiality and security are desired for the solution? How will the flow of data and information be managed?

CONDITIONS AND PROBABILITY OF ADOPTION BY BLOCKCHAIN TYPE	**<u>Scenario 1:</u>** ***Failure of public blockchains***	**<u>Scenario 2:</u>** ***Failure** of **private/hybrid blockchains***	**<u>Scenario 3:</u>** ***Cohabitation of** blockchains **without interoperability***	**<u>Scenario 4:</u>** ***Coexistence of** blockchains **with interoperability***
Time horizon(s)	Long term	Short or medium-term	Short or medium-term	Long term
Probability	Low	Average	Low / Medium	Medium / High
Completion conditions (cumulative)	- Political rejection - Legal rejection - Social rejection - Economic and commercial rejection	- Economic and commercial rejection - Political rejection - Social rejection - Computer rejection	- Computer rejection - Economic and commercial rejection	- Political acceptance - Legal acceptance - Social acceptance - Economic and commercial acceptance - Computer acceptance
	In the long term, it seems exist a low probability that blockchains public disappear in the in favor of those private/consortium um, due to discharges	In the short to medium term In the long term, it seems exist a probability than the average promises economical, commercial, policies, social and computerized	In the short to medium term term, it seems exist a low probability or average than the blockchains public, private and hybrids cohabit without being interoperable at them, because this	In the long term, it seems to exist a probability average or important than blockchains public, private and hybrids live together on markets and at multiple uses, from

Explanations and food for thought	successively political and social, legal, economic and commercial.	private blockchains and consortia fail in favor of from those public.	implies rejection of the search for interoperability IT (opposite at practices current market trends) so and a segmentation economic and commercial from every blockchain	complementary and interoperable. This rests on a acceptance political, social, economic and commercial so than IT, more or more or less long according to visit
			for markets and partitioned uses (this which is rare and applies à a minority of markets).	situations observed.

Title 2: Stable law in the face of constant technological and social change

Chapter 1: Law in the age of the digital society, between promise and challenge

In the 19th century, industrialization and technological progress were criticized for their economic, social, political and environmental impacts. These issues are still relevant today for all new technologies, including digital ones. In the early 2000s, IT was seen as a technical solution with no environmental consequences, since it was immaterial and cross-border, and because it was only supplied by a handful of technologically advanced players (thus masking certain social and ecological costs for society). It therefore seems important to distinguish technological progress from social progress, as not every technological advance systematically guarantees real social progress for society. Digital transparency must be verifiable in order to recreate digital trust with tangible proof for the benefit of citizens. Decentralized digital identity, which will be explored further in the second part of this study, and public blockchains, can be a source of major progress with beneficial economic and societal effects for individuals, provided their ecological effects are kept under control, for example with a "Low Tech" approach[481] . Each new digital technology represents a technical advance, but it is essential to assess it objectively in terms of the rules of law, which are themselves modelled on the needs of society.

1.1 Democracy and new technologies

Democracy is perceived as the emanation of a collective will, generally expressed through voting and elections. This collective vision of society is confronted by the growing individualism of people whose personal interests are sometimes at odds with a collective vision. The increase in personal demands[482] can, however, make it possible, with the possibilities offered by digital technology, to acquire a new collective power that can be transposed into the physical world (whistle-blowing, anonymous online voting, etc.). The unprecedented social interconnection made possible by digital technology also overturns certain traditional social processes, making it possible to

[481] V. Appendix 3, Focus 6.
[482] *Op. cit.* Presentation in this curve of the number of appearances of the term "identity" in literature from 1800 to 2019, available at the following address

digital emancipation of people and their identity (fundamental rights and freedoms, data, opinions). The utopian but widespread image of a participatory and direct democracy as in ancient Greece may become difficult to apply in today's context, given the rapid growth of the world's population coupled with the rise of identity and political demands. It seems that[483] democracy relies heavily on the freedom of expression of the different groups that make up a society, as well as on the legitimacy of the power in place and the presence of counter-powers working in principle for the general interest. This enables the population to govern itself by protecting the fundamental values essential to the common good[484] .

The new blockchain technologies and the decentralized digital identity mentioned above, which are the subject of a detailed study in the second section of this report, appear to be counterpowers at the service of certain fundamental freedoms. These new technologies, such as bitcoin and Ethereum[485] , are creating digital commons in the service of a digital society that is increasingly driven by Internet users, who can now question the role of certain institutional players. For example, banking and financial law is based on the need for intermediation, which Web 3.0 can do without. In fact, these new technologies enable a tremendous liberalization of acts by all communities, without any borders, which can structure themselves online to transmit and assert their messages and values. In theory, these new possibilities would enable a return to more direct democracy. Digitization and the decentralization of interactions offer Internet users a glimpse of new online social models, with fewer states and less trusted intermediaries. As a result, these new technologies are redrawing Jean-Jacques Rousseau's social contract[486] , conferring a new individual power of influence on people in their quest for personal autonomy, now well beyond the political and social power of the ballot box. So, while digital technology can enhance the exercise of democracy, it can also undermine it and give rise to anti-democratic behavior. Reference is made to illegal actions perpetrated and disseminated remotely by pseudo-anonymous Internet users, such as the mass dissemination of false information, behavioral psychometrics[487] , *deep fakes*[488] or digital rumors. For operators in the digital sphere, be they major technology companies or governments, the technical possibility of widespread surveillance of populations can gradually take precedence over the rule of law and democratic values, particularly in times of political transition.

---

[483] Term derived from the Greek "*dêmos*" for "*people*", "*daíomai*" for "*distribute*" and "*kratein*" for "*command*".
[484] MAALOUF Amin, "What is sacred in democracy are the values [human dignity], not the [political] mechanisms", *op. it. "Les identités meurtrières"*, p.178.
[485] V. Appendix 3 and Appendix 6.
[486] ROUSSEAU Jean-Jacques, "Du contrat social - ou principes du droit politique", available at
[487] This is the psychological study of Internet users' digital behavior. This new field, widely used by *Cambridge Analytica*, is now considered a new digital weapon by the European Commission. These platforms, originally created to connect us, are now becoming tools in the service of geopolitics.
[488] This is the animation of a photo or video using artificial intelligence to express words or behaviors that do not come from the targeted physical person, *v.* in this sense the recent photo of the Pope, "Cette photo du Pape en doudoune qui affole le web est un fake créé par l'AI", March 28, 2023, in *journaldugeek.com*.

major. Speaking at a conference at CERN in 2019, Internet founding father Sir Tim Berners-Lee wonders *"where is the balance between letting technology companies do their thing and regulating them? Where is the balance between freedom of expression and hate speech?* (...)" and continues "*oops! The web is not the web we wanted in every respect"*[489] . It seems that this dilemma between digital freedom and IT dependency is becoming more acute by the day, for example in view of the forthcoming adoption of a digital euro that is sometimes considered controversial and a source of concern by some digital experts.

While the decentralization of the Internet made possible by blockchain technology, coupled with the control of one's data enabled by the decentralized identity we discuss below, reflects the establishment of a possible direct digital democracy[490] , we must bear in mind that this digital utopia should not obscure the fact that representative democracy remains a realistic and rather balanced solution in view of the complexity of society. These technologies are often viewed with ambivalence, because on the one hand, they are seen as innovative means of unprecedented democratic involvement and participation online, and on the other hand, they are seen as tools that infringe collective rules and only benefit individualistic people. To maintain democratic foundations, we need to ensure that the rule of law institutes rights and duties for every citizen. Since IT theoretically has no rules other than those imposed by developer communities, the question arises as to whether the law shapes IT, or whether IT shapes the law[491] . Indeed, science and digital author Aurélie Jean reminds us that "*it remains true that algorithms and their protagonists influence the law indirectly (or not), given the complexity of the discipline, the lack of expertise of legislators in the field, and the power of tech giants*"[492] . In concrete terms, public blockchains appear to increase citizens' freedom of information, expression and communication, as seen, for example, with the creation, in the early days of the Internet, of an unprecedented digital version of the Journal officiel de la République française (JORF) and online public services. Freedom of the press and freedom of enterprise are therefore strengthened by the use of a public blockchain, especially in countries where the exercise of democracy is limited or non-existent. According to this demonstration, public blockchains have the potential to revolutionize developing countries by offering innovative solutions to the problems of corruption, transparency and financial inclusion. In these countries, corruption is endemic and it is the most vulnerable people who are most affected. Public blockchains can offer a solution by enabling the traceability of transactions of various kinds (financial, organizational, contractual) to be formed online and to be used by the public.

---

[489] Associated Press, "Father of World Wide Web Tim Berners-Lee says what his creation has become isn't the web we wanted ", in *dailymail.co.uk*, 2019, accessed at.

[490] Blockchain technology as an unforgeable digital register of data and decentralized identity as sufficient proof of citizenship.

[491] LESSIG Lawrence, "Code is Law: on liberty in cyberspace", in *Harvard Magazine*, 2000, *op. cit.*

[492] JEAN Aurélie, "Les algorithmes font-ils la loi?", in *Humensis*, 2021, reading position in the book: 94%.

an alternative for democratic expression. Consequently, the digitalization of social interactions implies a change in the exercise of certain fundamental rights and freedoms. This evolution must be supported to enable a more effective extension of online rights while remaining faithful to cryptographic and legal rules, in particular the RGPD Regulation[493] and the eIDAS Regulation[494] which are explored below. As a matter of principle, nothing should be more important in a democracy than the personal emancipation of its citizens. In a representative democracy, the state must train its citizens in the use of emancipatory technologies such as decentralized identity or the use of crypto-assets, for example. While citizens are condemned to be or become cybercitizens, it is up to them to choose the conditions for doing so, i.e. to decide, in complete transparency and confidence, how to use the new technologies made available to them.

1.1.1 Cyberspace as a place of sovereignty and legal autonomy

This study reveals an asymmetry between the exercise of people's rights in the real world and the exercise of those same rights in the virtual world. This form of distance and incompressible latency between the exercise of new technologies and the exercise of rights seems to be gradually intruding into people's digital lives over a period of time specific to each *phygital* identification situation. In reality, it's a never-ending race, as technologies constantly evolve, disrupt and outpace the law[495] . The notion of cyberspace is indeed a complex concept to define. It can be defined as an immaterial communication space created by a global interconnection between computers. A place for economic, cultural and, more broadly, social encounters, it represents a new virtual space, sometimes perceived by some Internet users as a digital territory[496] that would guarantee an informational space marked by freedom, transparency, sharing, equality and progress. In reality, it seems that the frontiers of this Internet web are not physical, but ideological and therefore infinite, with each person able to be in several places at the same time and instantaneously to carry out tasks as diverse as they are varied, with total freedom of navigation, a kind of digital freedom of movement. The use of the Internet and its new technologies leads us to revisit the concept of digital sovereignty with contemporary acceptance[497] . Rather than trying to propose a general definition of

[493] See *infra,* II, Title I, chap 2. 1.1
[494] See *infra*, II, Title 1, 2.1.1.1.
[495] V. Appendix 4.
[496] Since its creation, this new Eldorado and digital territory has been the subject of numerous geographical references, to describe it as "web browsing", "Internet ports", "information transiting through channels", and so on.
[497] BELLANGER Pierre, *La Souveraineté Numérique, op. cit.* 2014.

notion of sovereignty in the digital age, it seems more appropriate to evoke the following perspectives:

(i) Initially, a state's sovereignty was defined as its capacity for autonomous management of its population and territory. Although this capacity for control also extends to the digital sphere, it takes longer to be established due to the constant evolution of disruptive digital ecosystems that claim their own autonomy and sovereignty in IT, economics and politics. State sovereignty in the legal sense is thus struggling to assert itself in the digital sphere, and is tending towards a collective, national sovereignty aimed at ensuring the protection of Internet-user-citizens in the face of digital opportunities that sometimes generate short- and medium-term risks. In the following section, we mention that digital sovereignty is also associated with major technology companies, whose economic, technical, social and legal powers are constantly increasing, influencing society in both positive and negative ways.

(ii) As far as companies are concerned, sovereignty mainly refers to their ability to be independent and to have strategic room for maneuver due to their size and constantly changing social contexts.

(iii) For citizens and Internet users, sovereignty means personal or collective freedom of action and choice. However, this individualistic ability to influence one's immediate environment remains limited in comparison with previous definitions, as every online surfer is aware that his or her personal control, and by extension digital sovereignty, is limited and dependent on digital service providers. Despite this fatalism, which decentralized systems are designed to counter, some online services (e.g. video games, encrypted messaging) nevertheless promote this ability to self-define online. So, grouped together in communities, Internet users can create new conditions for the emergence of digital sovereignty for their community. This sovereignty is thus contextualized, but tends to grow in principle within the practical limits of respect for the legal rules protecting Internet users. In practice, this individual sovereignty is largely subordinate to a sufficient degree of mastery and understanding of digital systems, which today is the case for only a minority of Internet users.

Finally, the plurality of possible definitions for the concept of sovereignty means that it cannot be solely circumscribed to its statist, authoritarian or legal acceptance. It's a question of understanding this notion from an individual angle, that of digital existence and its mastery for the digital self-determination of individuals and in its entirety. In reality, it seems that

is moving towards a form of competition between several complementary definitions of the concept of digital sovereignty. It is likely that the traditional definition will persist due to the rule of law in developed countries, but there is no doubt that economic players will fight to defend their business models. However, this same struggle must not compromise the citizen-based definition of digital sovereignty that we support for the benefit of Internet users, and particularly those living under a rule of law perceived as weak in certain developing countries.

1.2 The short time of innovation versus the long time of regulation

Depending on their needs and situations, economic players want the law to apply either quickly, to their benefit, or over a longer period of time. Technological innovation is a seemingly short process, thanks to the technical and social revolutions it can rapidly engender[498] . Since data is always accompanied by other data or metadata, it should be considered as fluid rather than static. It is this fluidity, which is intrinsic to IT, that is at the root of the difficulties in grasping the notions of space and time, which are specific to IT, and which jurists sometimes encounter with difficulty[499] . But it seems that all technological innovation also requires a long preliminary period, often invisible to neophytes, which for a time is confined to a small circle of well-informed technophiles[500] . As mentioned in the previous sections, the Internet is in fact the fruit of several decades of IT and social development, and a similar observation can be attributed to the development of cell phones or digital identity, as mentioned above. So, if the time for innovation and the time for regulation both necessarily take a long time, how can we explain the gap in perception and temporal experience between the perceived rapid evolution of new technologies and the perceived long evolution in terms of applicable legislation? One possible explanation is that the complex and constantly evolving nature of innovation can only be fully understood and accessed by a small group of people, mainly developers[501] . Although open-source IT developments are publicly available, this social restriction linked to specific skills imposes a technical barrier that can only be overcome by certain events[502] which can lead to rapid dissemination and

---

[498] LASSEGUE Jean, GARAPON Antoine, "S'agissant du temps, le numérique détruit la durée vécue: (...) il contracte le temps d'un échange à presque rien [...]", April 11, 2018, "Justice digital", PUF, p.120.
[499] *Ibid*. "Innovation always claims to serve the law, but it also serves business, because (...) the two are inseparable [...]", p.99.
[500] See *above*, II, Title 2, 1.3.1
[501] De FILIPPI Primavera, WRIGHT Aaron, "Even though smart contract code is publicly available on the Internet for anyone to review, only a small number of people are capable of verifying that code," "Blockchain and the law: the rule of code," April 9, 2018, in *Harvard University Press*. Location 2759 of 7004.
[502] For example, when major technology companies decide to seize a new technology, adopt its standards and promote its merits, *see infra*, II, Title 1, 1.3.1.

of innovation in the public and social sphere, creating an exponential adoption that feeds on itself. In this respect, citizens and Internet users do not perceive these temporalities as long, but rather as lightning-fast, in line with the "*Fraisse's law*"[503] of French psychologist Paul Fraisse, known for his work on the perception of time. Thus, it is not innovation that is lightning-fast, but rather its social adoption, due to the phenomenal circulation of information via digital social networks[504] . In law, however, information is not intended to circulate rapidly, but rather to ensure compliance with texts and procedures whose conditions are duly identified and framed, in order to guarantee fairness and transparency before the law. This long process of regulation is the fruit of public discussions, both convergent and contradictory, in an attempt to provide the best possible framework for new technological phenomena impacting society. This initial process of gathering and exchanging information thus seems longer and more tedious[505] , in the face of the silent and seemingly faster pace of innovation. While lawyers and developers are both passionate professions in this respect, it has to be said that emotion is not managed in the same way in these two ecosystems: being a lawyer means concentrating on the legal rules to be established, whereas developers give free rein to their personal emotions when programming IT rules, for which only end-users will be biased judges. The purpose of these few observations is not to demonstrate that the slowness of regulation is detrimental to innovation. Quite the contrary, the aim is to understand why structural differences exist, and how they can be articulated together despite their persistence. Ultimately, it's about considering that (long) time is not (fixed) duration. In other words, regulation must give innovation time to work its magic, with a minimum of legal supervision due to the legal rules[506] to be put in place, before eventually establishing appropriate regulation over a clearly defined period of time. In this way, the timeframes of innovation overlap without confronting each other, thanks to a distancing of their respective temporalities.

"(...) *if the law is often conservative due to its establishment often out of step with social and economic practices, it must anticipate scenarios and technological, medical or even societal changes as best it can in order to endure. It should be pointed out that the RGPD appeared ten years after the creation of Google*"[507] . Finally, while innovation is undeniably a source of upheaval for the law, legal experts must try to identify

[503] This law, named after the French psychologist who enunciated it, assumes that the more passionate and pleasurable we find a task to accomplish, the shorter the notion of time seems to us: "The more unity a task has, the more interesting it is likely to seem. Unity reinforces motivation (...). The more unity a task has, the shorter it appears", FRAISSE Paul, "Psychologie du temps", 1975, Ed. PUF.

[504] WOITIER Chloé, "Elon Musk et des centaines d'experts réclament une pause dans l'AI, évoquant 'des risques majeurs pour l'humanité'", March 29, 2023, AFP Agence, in *Le Figaro*.

[505] JEAN Aurélie, " Les lois s'inscrivent par définition dans les temps longs. The law is even generally perceived as conservative insofar as texts often arrive out of step, not to say behind the times, with social practices", online version in *decitre.fr*, Ed. Humensis, 2021, reading position in book: 8%.

[506] *Ibid.* "As the RGPD has succeeded in doing, let's make time an ally and not a threat through legislation that authorizes while strictly framing and severely repressing", Reading position in the book: 66%.

[507] *Ibid.* Reading position in the book: 65%.

and then anticipate when mass adoption by society is likely to occur, which means training in 2.0 and then 3.0 technologies. Crypto-assets (public blockchains), for example, are well on the way to reaching this pivotal adoption point, while private and hybrid blockchains have yet to do so, as has decentralized identity, as discussed below.

1.3 Protecting online freedoms: the right to privacy and digital integrity

Eight years ago, the founder and chairman of the Skyrock media company wrote in a book that "*the painless capture of our private lives in return for services, however attractive they may be at the outset, is today a deceptive gratuity whose future price is not even quantifiable, given the impact it will have on our lives*"[508] . However, this observation is gradually being called into question by Internet users and legislators alike, with the adoption of various laws dedicated to data protection. The right to privacy is a fundamental right that must be exercised by all Internet users. It is essential to their autonomy and, more generally, to the protection of human dignity[509] . It allows other fundamental freedoms to be linked to it (freedom of worship, expression, etc.). As a matter of principle, "*what is illegal offline must also be illegal online. European values and ethical rules, as well as social and environmental standards, must also apply in the digital space*"[510] . Technology has always been intimately linked to people's rights. For example, our ability to protect privacy is now greater than ever thanks to various digital tools[511] and cryptography, including the ZKP[512] studied in the second part of our research, although surveillance capabilities are proportionally equal or even greater than before, depending on the country and social and cultural doctrines adopted. It is now possible to uniquely identify individuals among the masses of data streams in the digital universe, which can compromise their ability to make conscious or unconscious decisions and uses. Some organizations, companies and governments, have the ability to monitor every conversation, every business relationship and every place visited. These capacities, latent or exercised, can have negative effects on individuals, groups and society in general, as they can curb the actions of citizens, exclude and discriminate against individuals. In other words, these organizations have the power to influence the way individuals think about and manage their relations with markets and the various branches of the rule of law, sometimes w i t h o u t the people concerned being aware of it.

---

[508] BELLANGER Pierre, "La Souveraineté Numérique", 2014, *op. cit.* Locations 2315 and 2331 on 3565.
[509] V. Art. 6 of the 1789 Declaration of the Rights of Man and of the Citizen: "All citizens being equal (...) are equally eligible for all dignities (...)".
[510] *Op. cit,* CE, "Communication shaping europes digital future", *op. cit*, consulted online December 20, 2021, p.6.
[511] Mooc Inria, ICN-SNT-Python, 2019-2021, "[...] information and communication technologies (ICT) are not definitively and indubitably threats to privacy. It is indeed also possible to design new techniques to protect privacy and resolve the kind of hiatus evoked with big data", in *Informatique et culture scientifique du numérique*, p.67.
[512] *See infra*, II, Title 1, 2.2.6.1.

[513] . The growing adoption of centralized services and technologies is gradually leading to a loss of control and a certain ignorance of the widespread surveillance of which Internet users may be victims. The latter often have little computer knowledge to question the foundations of this surveillance. One of the essential components of the right to privacy is the right to protection of personal data, and certain international instruments contain specific legal provisions to this effect[514] . The right to privacy is often regarded as intangible, which may lead some people to think that their privacy is not important, because they would have nothing to hide, but this would be tantamount to saying that they do not consider other rights such as those relating to freedom of expression or freedom of the press simply because they have nothing to say or write.

According to French author and philosopher Gaspard Koenig[515] , the programmed disappearance of free will in the digital sphere is the subject of a theoretical consensus. At the same time, the work of renowned American-Israeli economist and psychologist Daniel Kahneman, according to whom the individual is constantly confronted with his or her own illusions and cognitive biases, coupled with the work on behavioral influence ("*Nudge*"[516]) by economist Richard Thaler, as well as the neuroscience research of French neuropsychologist and author Stanislas Dehaene, tend to confirm that people's online identities are altered, even alienated, by major digital companies. From the point of view of Internet users, it is no longer just the State that could be considered the enemy of respect for the rights to privacy and freedom online[517] , but also and above all certain large technology companies. The sophisticated digital tools of large private technology companies contribute to an erasure of people's individualities, which means that the more individuals lose their singularity, the less able they are to claim a free and democratic identity. Faced with this manipulation of data and transposition of identities, it's not a question of condemning and avoiding new technologies, but of appropriating them. The role of the State is to empower individuals, i.e. to provide them with the technical means to reclaim their digital data and identities. Thus, privacy must be secured by default and by design, thanks to new technologies and mechanisms that are more respectful and less data-intensive. This technological and legal protection must be guaranteed by major technology companies as well as by governments, which are not yet sufficiently encouraged to do so by citizens and Internet users alike.

---

[513] Le Monde AFP, "Espionnage de journalistes et d'opposants : l'affaire 'Pegasus' provoque l'indignation", November 4, 2022, in *LeMonde.fr*

[514] *See* in particular: art. 14 of the UN Convention on Migrant Workers, art. 16 of the UN Convention on the Rights of the Child, art. 10 of the African Charter on the Rights and Welfare of the Child, art. 4 of the African Union Principles on Freedom of Expression (right of access to information), art. 11 of the American Convention on Human Rights, art. 5 of the American Declaration of the Rights and Duties of Man, arts. 16 and 21 of the Arab Charter on Human Rights, art. 21 of the DDH, art. 8 of the ECHR.

[515] FERRY Luc, in *Le Figaro*, online, published October 23, 2019, accessed November 18, 2021.

[516] "Nudging" consists in encouraging people to make certain unconscious decisions, using psychological incentive mechanisms. The aim is to lead them in a certain direction, for their own good or for the collective good, depending on certain circumstances. ELIE Pauline, "Beware the tyranny of nudges. Les "nudges" vous voulez-ils (vraiment) du bien?", 2022, available at the following address

[517] ECHR, "Mass surveillance - factsheet", 2022, available at

themselves. At present, computer science and legal research are largely regarded as independent subjects. This situation creates legal uncertainty for entities seeking to process pseudo-anonymous datasets (discussed in the next section), and may even lead to widespread terminological confusion for the general public, who nonetheless benefit from such protection and mechanisms that are thus beyond their reach. In reality, the General Data Protection Regulation (GDPR) already mentioned, does not seem to fully meet expectations in terms of personal data protection. Privacy should be a guaranteed and easily accessible right when using websites, not an action that users must seek to exercise through lengthy and sometimes costly procedures. Since 2021, several Swiss jurists have been proposing the adoption of a new right to digital integrity[518] . Their ambition is to develop a new fundamental right to digital integrity, i.e. a few general and impersonal principles that everyone can understand and enforce. In addition to the mental and physical integrity of the human person, the aim is to include and guarantee a new digital dimension that would stem from this initially physical protection. For example, during a face-to-face vote, it is difficult for a person to be influenced by the public nature of the voting process (various procedures ensure the integrity of each citizen's vote, such as the voting booth). On the other hand, when voting online and a person is alone in front of his or her screen, all it takes is for other Internet pages, such as Facebook or Twitter, to be visible for any direct or indirect influence to occur and violate the voter's digital integrity. In this example, guaranteeing a voter's digital integrity means guaranteeing that person's free online self-determination. In this respect, and as proposed by legal experts, Article 3 para. 1 of the EU Charter of Fundamental Rights[519] , could be amended as follows: "*Everyone has the right to respect for his or her physical, mental and digital integrity*" (here added and underlined). In reality, if the right to privacy is not respected, all a person's other rights may be threatened. As lives become increasingly digital, the right to privacy could be extended, and at the very least include all the actions of a life that has now become digital.

1.3.1 Contextual pseudo-anonymity and residual anonymity in Web 3.0

On the Internet, end-to-end encryption is necessary and essential to ensure confidential browsing for Internet users. Without these encryption mechanisms, service providers are able to reconstruct, categorize and market the online choices and behaviors of

[518] GUILLAUME Florence, MAHON Pascal, ROUSSEL Alexis, "Réelle innovation ou simple évolution du droit? le droit à l'intégrité numérique", Université de Neuchâtel, Éd. Helbing, Lichtenhahn, 2020, p.180.
[519] V. Art. 3 of the Charter of Fundamental Rights of the European Union: "Everyone has the right to physical and mental integrity", consulted on April 11, 2022, at the following address

Internet users[520] . If all online services could be trusted to preserve the confidentiality of their users' information, these encryption mechanisms would not be necessary. But they have become necessary as the Internet and the online services and data it hosts have developed. Indeed, if "*one of the fundamental freedoms brought about by the Internet lies* (...) *in its capacity to undo the burden of responsibility imposed by the automatic assignment of the right of expression to an attested identity*"[521] , it has to be said that some Internet users abuse this online confidentiality, i.e. the anonymity conferred by these encryption methods. Indeed, because their content is encrypted and their identities more or less temporarily masked, some Internet users enter into illegality through their online actions or behavior, and there is no way of distinguishing them from all the other encrypted and legitimate content circulating in the mass of computer systems. The risk is therefore to lose cryptography as a tool for protecting privacy, in the name of the fight against a minority of online malicious actors. The challenge is to find cryptographic mechanisms that can separate harmful content from legal content, without encroaching on user confidentiality. Today, the concept of *anonymity* is largely dependent on social, ideological, IT and cultural models. In the Middle Ages, it was a non-derogable rule in literature for all religious authors (especially copyist monks), whose main task was simply to copy and distribute works without copyright or personal appropriation. With the development of printing, the 17th and 18th centuries saw the revelation of the individual and literary identity of authors, whose anonymity became not a condition, but a refuge against political, religious or social censorship. The use of a pseudonym to preserve anonymity was common practice, and for some writers, authors or philosophers, it was a way of concealing themselves, such as the name Voltaire[522] taken by François-Marie Arouet in 1718 after his imprisonment in the Bastille, or George Sand[523] taken by Aurore Dupin de Francueil as her real surname. Over the last few decades, following a series of scandals involving data leaks, theft and manipulation, the younger generations of Internet users seem to be gradually seeking new forms of online anonymity[524] . But the advent of digital technology is transforming the concept of anonymity. While it is relatively easy to remain anonymous in the physical world, it has become almost impossible online. Any use of computer equipment and browsing on the Internet leaves digital traces that can be retrieved, recorded or exploited, which is not the case in the physical world, where it is currently simpler to preserve anonymity.

[520] Messages, photos, videos, Internet browsing, etc.
[521] GAYON Jean et al, "L'Identité: dictionnaire encyclopédique", *op. cit.*
[522] "Voltaire, le jugleur de lettres (1/2)", in *The Voltaire Project,* 2015, accessed online on December 20, 2021.
[523] Wikipedia, "George Sand", accessed online on December 20, 2021.
[524] DUFOUR Fanny, June 26, 2022, "(Re)devenir anonyme sur Internet, la nouvelle tendance des années 2020?", Clubic.com. Retrieved June 27, 2022, from

and assert ideas anonymously, for example at a demonstration[525] . In the digital world, it is therefore more accurate to speak of the *pseudo-anonymity* inherent in any identity that has become cryptographic (transactions thanks to cryptographic tools) or digital (IP address, for example), such as a bank IBAN and BIC enabling a sequence of alphanumeric characters to identify the author of the transaction. Today, certain software programs offer *more* or less relative *pseudo-anonymity*, such as Tor Browser, which can be used to increase freedom of information and expression in countries where censorship is a daily reality[526] , or to access illicit markets under cover of anonymity[527] .

Anonymity therefore allows total concealment of identity, whereas *pseudo-anonymity* within the digital universe only allows a certain form of online concealment. It therefore seems more appropriate to consider the concept of *pseudo-anonymity* rather than *anonymity* within the digital universe. Although the idea of complete anonymity today represents a conceptual utopia in computing, this doesn't mean that a rare few savvy Internet users don't manage to live without ever being identified, like some hackers[528] . Nearly 12,700 fake[529] accounts with images generated by artificial intelligence (AI) tools are said to have been created on LinkedIn since the beginning of 2023, with the creation of a "Bot" (software) that generates likes and requests. Some Internet users can therefore take advantage of their temporary anonymity on social networks to influence certain online communities using multiple accounts, IP addresses and digital identities. This so-called "*astroturfing"* technique, also known as a "*Sybil attack*" in computer science[530] , aims to anonymously manipulate, polarize and increase a reputation or membership on a digital network en masse. This phenomenon has always existed on digital networks and will probably continue to do so, as anonymity is necessary[531]

---

[525] While social anonymity is predominant in our physical world when a person is walking down the street, the proliferation of biometric identification systems calls this anonymity into question in the real sphere, as people can be solicited at any time, subject to compliance with a legal framework (accidents, theft, terrorism, etc.).

[526] The New York Times uses Tor software to bypass online censorship in countries where access to information is restricted or prohibited. Tor is a decentralized network of relays (computers) that masks the user's IP address and encrypts traffic, making Internet browsing virtually anonymous and secure. By using Tor, The New York Times can provide more secure and private access to its readers in countries where press freedom is restricted. It also enables journalists and sources to communicate more confidentially without fear of surveillance or censorship. In short, Tor is an essential tool for media seeking to guarantee freedom of expression and protect journalists and sources. For more information, see the Research Brief "Methods of legalizing and laundering mafia activities", published in July 2020, accessed August 2021 and available at.

[527] Illicit online marketplaces, also known as *darknets*, are hidden websites that can only be accessed via the aforementioned Tor network. The Tor network enables buyers and sellers to remain anonymous by masking their IP address and encrypting their traffic. Transactions are often carried out using crypto-assets to avoid leaving any traces. Although using Tor is not illegal per se, these illicit platforms are often associated with the sale of drugs, weapons, counterfeit goods and other illegal products. It is important to note that using Tor does not guarantee complete anonymity, and that authorities may be able to track transactions and identify users using more or less sophisticated surveillance techniques.

[528] PARGAMIN David, "Sur la piste des voleurs de cryptomonnaies", in *Challenge*, n°779, March 23, 2023, p.46-47.

[529] BODNAR Bogdan, "That's it, the first AI-generated scams are online", February 23, 2023, in *Numerama*, available at

[530] V. Appendix 6, Focus 1.

[531] BABEAU Olivier, President of the Institut Sapiens, "Face à la tyrannie de la transparence, retrouvons les vertus de l'opacité", published May 4, 2021, in *Le FigaroVox*, Chroniques.

in some cases, and wanting to eradicate it may well be undesirable as well as utopian. Social networks also represent a wonderful opportunity to share personal experiences without fearing for one's physical and personal safety, thanks to pseudo-anonymity, reinforced today by social networks such as Facebook, Twitter and Instagram, which offer their subscribers[532] the assurance of the authenticity of their messages and content, for a monthly fee of $8 for Twitter and $11.99 for Facebook. The *search for anonymity* online can be seen as a deviance by some legal experts "(...) *chaos results from anonymity*"[533] , while the end of anonymity online would mean an obligation for all Internet users to claim authorship of their words.

Because online anonymity actually encourages antisocial behavior such as harassment, defamation, slander, mockery, insults, hate speech and identity theft, many governments are gradually seeking to put an end to it. Yet this political will seems paradoxical, as the terms *anonymity* and *pseudo-anonymity* create a form of legal and IT confusion for the general public. Whenever anonymity is called into question on the above grounds, it seems to be to offer short-term advantages to Internet users, such as high transaction traceability, or to combat money laundering and the financing of terrorism. The impossibility of being *pseudo-anonymous* means increased digital identification, based on widespread suspicion of fraud, jeopardizing fundamental freedoms. On a psychological level, *pseudo-anonymity* offers a person the opportunity to defend his or her positions (political, social, economic) under a pseudonym that protects his or her integrity. It can also enable the author to acknowledge his or her mistakes and return to online exchanges under a new pseudonym, freed from any social judgment thanks to his or her pseudo-anonymity see anonymity. In theory, this freedom of expression without judgment or attachment to a recognizable identity allows Internet users to be more open in their thinking. However, social influence can, on the other hand, encourage some users to cling to their positions, which can lock them into their own thinking (identity fiction), thus creating the paradox of social networks: both emancipators and social executioners.

But shouldn't *pseudo-anonymity* be a matter of contextualization and proportionality (as the following illustration suggests)? Everyone must accept that citizens and Internet users can act in the shadow of online anonymity, as some jurists have argued: "*the great sun of perpetual identification* [the end of anonymity] does *not illuminate: it blinds. It does not illuminate: it burns*"[534] . A society that controls a priori all individual behavior contributes to locking people up.

---

[532] " Les réseaux sociaux font payer la fin de l'anonymat ", in *Challenges*, n°776 of March 2, 2023, p.34.
[533] More precisely: "It is distressing that this vector of communication (e-mail, tweets, chat, forums, etc.), so easy to use, so vulgar in use, the primary means of exchanging information and a tool for social bonding, has become, thanks to electronic anonymity, the privileged terrain of cybercriminals: it is time to rethink the law and create the means to identify actors working on the networks", *op. cit.* BENSOUSSAN Avocats. "L'identité numérique 5.0". Lexing, p.47.
[534] NETTER Emmanuel. "L'identité à l'épreuve du numérique", in Larcier, 2020, p. 9, available at the following address

This is the case in China. However, it is utopian to think that a totally anonymous Internet would be viable, if only with regard to online commerce, which by design requires the legitimate collection of certain personal data such as a delivery address, surname, first name, age, and so on. While anonymity theoretically ensures pure confidentiality online, it does not always inspire confidence, particularly in the case of certain social transactions that require third-party trust through identification in order to guarantee the process and validity of digital exchanges.

From an IT point of view, public blockchains are designed to offer anonymity by design[535] , but the complete transaction history of crypto-assets, for example, remains publicly accessible online[536] . These principles of anonymity[537] and decentralization of exchanges are essential to guarantee the incensurability of a blockchain, i.e. the theoretical immutability of its transaction register. If the address of a crypto-asset wallet is identified, it is possible to trace the user's entire transaction history, which could pose a danger to his or her privacy and digital integrity. However, these same features can be used by analytics companies specializing in blockchain analysis (in consultation with law enforcement agencies) to identify parties involved in one or more illicit transactions, by examining ancillary information such as online forum posts associated with transactions[538] . Faced with the political will to enable systematic identification of crypto-asset users in order to trace the origin of their transactions[539] (e.g. when crypto-assets are "*dyed*"[540]), the following question arises: could this legally justified political will to systematically identify public blockchain players by putting an end to the pseudo-anonymity of transactions jeopardize their existence? Indeed, it seems that there is a vital risk for public blockchains to be confronted with these mechanisms for systematically identifying

[535] A public blockchain allows any Internet user to become a pseudo-anonymous user (via an address and a unique digital identifier, known as a "public key"), or to become an anonymous network validator by purchasing a specific computer dedicated to network validation, known as an "ASIC".
[536] V. Mempool - Bitcoin Explorer, 2022, to consult the Bitcoin blockchain in real time at the following address
[537] Anonymity plays an essential role in preserving the decentralization of a blockchain by allowing users to participate without having to submit to a central authority. It also avoids any risk of surveillance and censorship. In addition, anonymity encourages the adoption of public blockchains, as users feel safe carrying out pseudo-anonymous transactions. Finally, user anonymity promotes competition by enabling new players to participate without fear of being monitored or blocked by established players.
[538] In 2022, a new legal mechanism emerged in response to a theft of crypto-assets by hackers: the plaintiffs' law firm decided to send court documents (in the form of NFTs) directly to the pseudonymous addresses of the anonymous perpetrators in order to notify them of the existence of an investigation against them : "This gives us a mechanism to at least serve legal process on someone who controls an implicated address regarding a digital asset that has been affected," said Andrew Balthazor of Holland & Knight. In *New Approach*, "Big law firm uses NFT to serve court papers on anonymous defendants", June 17, 2022, in *Daily Business Review*. Retrieved June 18, 2022, from
[539] KRYPTOSPHERE®, June 27, 2022, "Contrary to popular belief, Bitcoin is NOT anonymous...", in *Cryptoast*, accessed June 28, 2022, at
[540] *Tainted coins are* digital tokens suspected or identified of being involved in an illicit transaction (money laundering, illegal activity, etc.). For further information, *see* I, Title 2, 1.4.1 *below.*

stakeholders in their ecosystems[541] (users, businesses). While public blockchains are designed to be decentralized, transparent and open, the use of *tainted coins*[542] is attracting the attention of authorities and regulators, although this illegal use of these computer protocols by some users remains marginal. Regulators may indeed require all crypto-asset exchange platforms and other service providers to identify and declare users transacting with these tokens, which may compromise the privacy and anonymity of other legitimate users on these blockchains. Moreover, this regulatory identification of these ecosystem players can also discourage innovation and development of public blockchains, as startups and developers may be reluctant to build on protocols where the regulatory oversight would be too restrictive.

To mitigate this risk, some blockchains such as Bitcoin and Ethereum[543] - studied in the Appendix - are developing privacy-enhancing technologies that enable users to carry out transactions anonymously or pseudo-anonymously, depending on the situation, while complying with regulatory requirements. Striking a balance between regulatory compliance and preserving the decentralized, pseudo-anonymous nature of public blockchains will take time and ongoing IT development. These remarks call into question the argument of the proclaimed anonymity of blockchains, today closer to a *pseudo-anonymity* as just explained and which has been criticized since the beginnings of Bitcoin technology[544] . The search for *pseudo-anonymity* for the developers of these protocols will remain a priority in this ecosystem[545] . Removing the principles of transaction anonymity and decentralization from public blockchains would also hinder the development and mass adoption of public blockchains and, by trickle-down effect, of their ecosystems, including private and hybrid blockchains. Consequently, the development of *pseudo-anonymization* mechanisms that respect the fundamental principles of blockchain (pseudo-anonymity and decentralization) can only be beneficial for this technology and the digital identities it hosts. It is argued that the right to *pseudo-anonymity* should be preserved on public blockchains, even on the margins and as an accessory to the anonymity already used by certain uniquely skilled developers known as "core" developers, who are indispensable for updating blockchain protocols.

---

[541] V. Appendix 7.
[542] For further information, see I, Title 2, 1.4.1 *below*.
[543] V. Appendix 6 Focus 2.
[544] "The network is robust in its unstructured simplicity. The nodes all work at the same time with little coordination. They do not need to be identified, since messages are not routed to a particular location and need only be delivered where possible. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as evidence of what happened while they were away. They vote with their CPU proof-of-work, expressing their acceptance of valid blocks by working to extend them, and rejecting invalid blocks by refusing to work on them. All the necessary rules and incentives can be applied with this consensus mechanism", NAKAMOTO Satoshi, "Bitcoin Whitepaper, Bitcoin: A Peer-to-Peer Electronic Cash System", accessible online at the following address, p.3.
[545] "Blockchain has thus enabled the emergence o f faceless, leaderless, totally autonomous entities.", *op. cit.*
"Monnaies, banques et finance: vers une nouvelle ère crypto Un enjeu de souveraineté et de compétitivité économique, financière et Monétaire", p.30.

public. To date, one of the Internet's best-kept secrets concerns the identity of the creator(s) of the Bitcoin protocol[546] , whose anonymity has persisted for over 14 years. While it would be unthinkable in the 21st[e] century to propose a disruptive new technological concept without revealing the identity of its creators, the mysterious origin of the Bitcoin protocol belies this observation. All we know for sure about this mysterious creator is his pseudonym:

"Satoshi Nakamoto"[547] . Nakamoto is said to have come into contact with the influence of the "cypherpunk" movement[548] , so much so that it is highly probable that he was active there under various pseudonyms before inventing and then unveiling the Bitcoin protocol on the Web[549] . Today, several plausible scenarios have been put forward for the inactivity of this mysterious figure(s) since 2010: voluntary retirement from involvement, death, loss of his cryptographic keys (enabling access to his Bitcoin funds)[550] , silent observation, government arrest, and so on. If doubt must persist to ensure the longevity of this computer protocol, it would appear that the individual or individuals behind the Satoshi Nakamoto persona have voluntarily decided to withdraw from the public eye. This decision may have been influenced by an invitation from Satoshi Nakamoto's former right-hand man, Gavin Anderson, to present the beginnings of Bitcoin to the CIA, an invitation which was refused by Satoshi Nakamoto. Since that day on December 12, 2010[551] , this is likely to be the last verified and public digital correspondence issued by Satoshi Nakamoto's pseudonym[552] (a year later, an email to Gavin Andresen would seem to confirm that anonymity was a fundamental element for Satoshi not to be compromised)[553] .

---

[546] According to a recent study: "64 agents mined most of the bitcoins between the launch of bitcoin and the moment when it reached the same price as the US dollar. We exploited data leaks to build a map of the blockchain in early 2011, in which bitcoins are ranked according to the agent who mined them", BLACKBURN Alyssa et al. "Cooperation among an anonymous group protected Bitcoin during failures of Decentralization", p. 64 of 76, available at.

[547] The main online profile of this pseudonym and character is available at the following address

[548] "Cypherpunk" is a buzzword coined by renowned author and hacker Judith Milhon. The term derives from a combination of the English words "cypher" (in reference to an encryption algorithm) and "cyberpunk" (in reference to an encryption algorithm).

"which stands for dystopian science fiction. This simple definition characterizes the ideology of this group of individuals and activists in the service of a free Internet that respects the privacy of Internet users (an ideology today more topical than ever). We note that encryption is the centerpiece of this movement, which is the cradle of many of the members and participants in the launch of the Bitcoin blockchain: the mother of all blockchains, based on a technological ideology that has only partly become a reality. On a political level, this movement marks its opposition to the omnipotence of states: "We Cypherpunks are dedicated to building an anonymous system. We defend our privacy with cryptography, an anonymous e-mail system, digital signatures and electronic money". From the article "À la découverte du mouvement cypherpunk à l'origine du Bitcoin", in *Cryptoast*, available online.

[549] In this respect, Satoshi Nakamoto drew on previous knowledge gained from work previously carried out (*B- Money, DigiCash, Hashcash*) by other IT experts (including Jean-Jacques Quisquater) present in the *"Cryptography mailing list*" to integrate them into his proposal: *The Bitcoin Project*

[550] V. Appendix 3.

[551] "Added some DoS limits, removed safe mode (0.3.19)", 2010, in *bitcointalk.org,* accessed 01/06/2022 at

[552] Except for a September 8, 2014 message allegedly posted by Satoshi Nakamoto according to a video investigation available at Barely Sociable. 2020. "The Most Elusive Identity On The Internet - Pt. 2" [Video]. YouTube. [553] Satoshi's last correspondence, an April 26, 2011 email to Gavin Andresen gave rise to another theory about the reasons for his abrupt departure. He wrote: "I wish you wouldn't keep talking about me as some mysterious shadowy figure, the press is just turning this into the prism of a virtual currency hacker. Maybe you should instead talk about the open source project and give more credit to your contributors and developers; it helps motivate them", "Satoshi's Final Email to Gavin Andresen". June 26, 2011, in *Nakamotostudies.Org.* Accessed June 20, 2022, at

According to Professor Emeritus of Mathematics and Cryptography Jean-Jacques Quisquater (quoted in the white paper and PDF formalizing Bitcoin)[554] , engineer and computer doctor Adam Back and several others, all publicly or otherwise associated with the Cypherpunks movement, were behind the birth of Bitcoin (perhaps sharing the pseudonym "Satoshi Nakamoto"). Indeed, it seems unlikely that a single person could have conceived the Bitcoin protocol, as this would have required multiple skills in software development, cybersecurity, IT infrastructure management, game theory[555] and very advanced economic and financial knowledge for the time. While there are many hypotheses concerning the identity of this mysterious genesis[556] , it should be noted that these attempts to unmask the identity of Satoshi Nakamoto remain unsuccessful to this day, counter-indicated by his community[557] , for reasons that seem rather legitimate in the light of the preceding remarks. Despite the speculation surrounding Satoshi Nakamoto's identity, it is undeniable that the anonymity of this pseudonym has enabled Bitcoin to give birth to a new class of technology unprecedented on the Internet: blockchain technology[558] . In other words, if Satoshi Nakamoto's identity had been revealed, the world might never have experienced the digital trust revolution represented by Bitcoin, as well as blockchain technology in all its forms, including private and hybrid. Indeed, Satoshi Nakamoto's identity could have been influenced by third parties or even pursued or stopped by a government, not least because of the proven links at the time between bitcoin and money laundering. This case study shows that *anonymity* can play an important role in the innovation of computer (social) networks. To achieve total decentralization, the entity or person at the origin of the network, generally centralized at the outset by a few developers[559] , must

---

[554] This means that Jean-Jacques Quisquater directly inspired the work of Satoshi Nakamoto as early as 1999, in addition to having helped organize events in London on behalf of the *Cypherpunks*. Privileged one-hour discussion with Jacques Quisquater at the *Forum International sur la Cybersécurité (FIC)* on 09/10/2021 about the Bitcoin protocol, decentralized identity and the identity of Satoshi Nakamoto.

[555] V. Appendix 6, Focus 4, 5 and 6.

[556] Numerous personalities claim to be Satoshi Nakamoto or to have unmasked his or their identity, which is indeed a *fallacy*, since it's all about clues and not irrefutable proof. Following our research, here is a serious, but non-exhaustive, list of candidates and people likely to be, individually and/or collectively, Satoshi Nakamoto (note that many of these people are attached to the aforementioned *Cypherpunks* movement): David Lee Chaum, Craig Wright, Paul Le Roux, Adam Back, Nick Szabo, Hal Finney, Tony Spilotro, Zooko Wilcox-O'Hearn, Len Sassaman, Gavin Andresen, Jed McCaleb, Shinichi Mochizuki, Neal King, Vladimir Oksman, Charles Bry, Wei Dai, Ian Grigg, Dave Kleiman. For further information, see the following sources: "Le mystère Satoshi: enquête sur l'inventeur du bitcoin", ARTE. 2021. YouTube. Available at; MoneyRadar Crypto. 2022. "Satoshi and the mystery of the Cypherpunks" [Video]. YouTube. Available at; Barely Sociable. 2020. "Bitcoin - Unmasking Satoshi Nakamoto". YouTube. Available at Wikipedia contributors. 2022. "Satoshi Nakamoto", available at

[557] Revealing Satoshi Nakamoto's identity would be tantamount to renewing and conferring economic, legal and social responsibility on this person. This new assumption of responsibility could lead to a loss of trust and, by domino effect, a loss of value for this 3.0 asset. The community therefore does not wish to respond to this legitimate curiosity, which would in fact be counterproductive for the entire blockchain ecosystem.

[558] See *below*, I, Title I, 2.3

[559] Any nascent computer network is by design computationally centralized, including Bitcoin in its early days. Indeed, it has been shown by researchers that Satoshi Nakamoto was running around 48 computers at the start of Bitcoin's launch, then gradually reduced this number, i.e. his computing power, as more *miners* joined the network (as he considered the network robust enough to allow himself to withdraw personally).

"We suspect that Patoshi consisted of at least 48 computers, with one machine for coordination and others on standby in case o f attack, which would explain the missing range of [10-18]. As soon as Satoshi judged the network

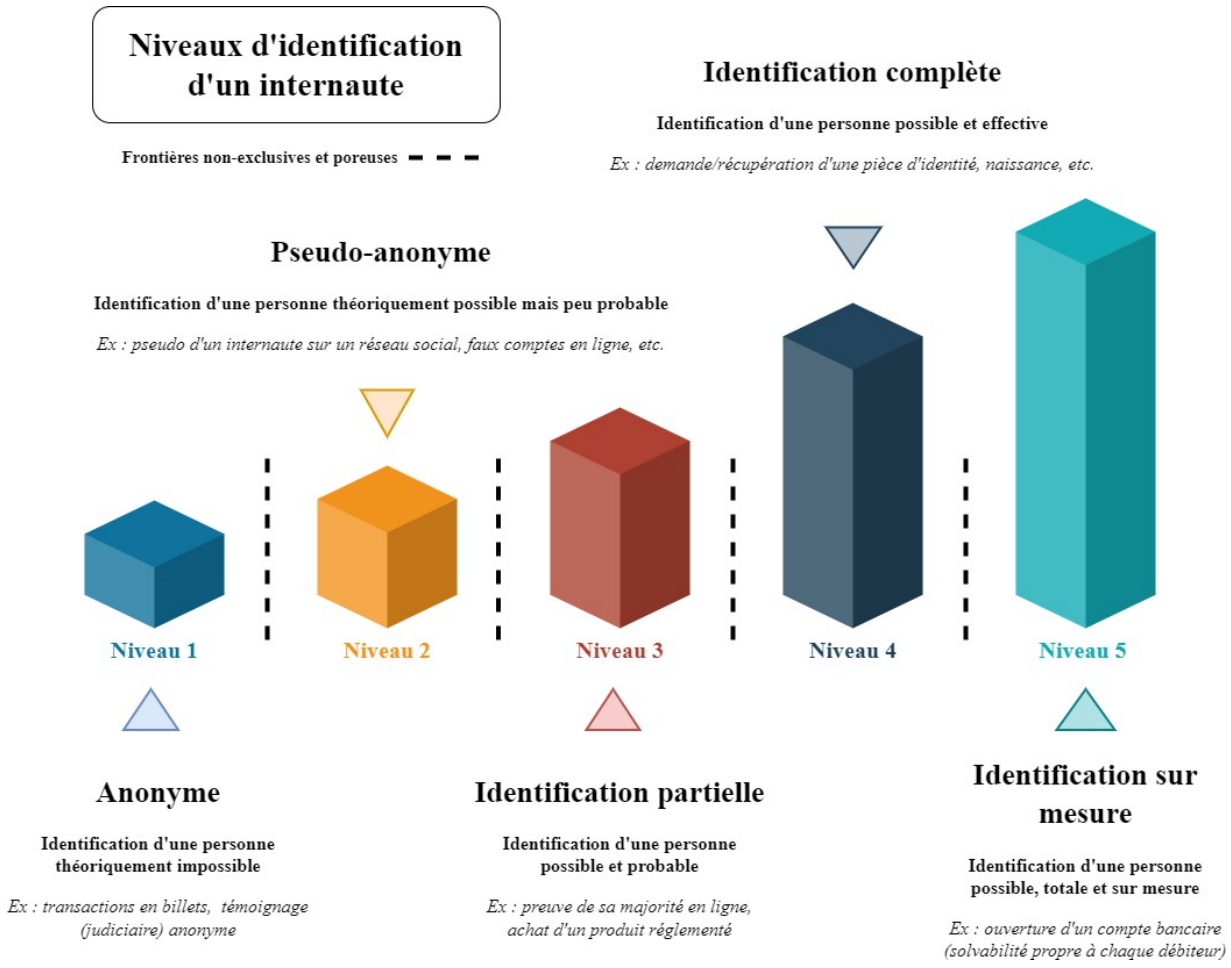
remain anonymous to avoid any risk of intimidation of the founder. In this respect, it is emphasized that the creation of a crypto-asset is not illegal, as the 900 or so people who have contributed to the development of the Bitcoin protocol since 2009[560] would have been prevented from doing so if anonymity had been lifted. For the[561] crypto-asset sector, *anonymity is* not seen as a requirement, but rather as an essential and structural historical feature. Conventional financial and institutional players regard this market as opaque, or as the source of a significant loss of confidence compared to other, reputedly more transparent, financial asset classes. But a certain minimum level of *anonymity* must remain possible, as it is a driver of innovation for its beneficiaries, who have the choice of seizing or divesting it at any time. Finally, because guaranteeing *anonymity* online seems technically utopian for the majority of Internet users, an intermediate solution - *pseudo-anonymity* - should be favored, and in an industrial way, i.e. through the use of programmed pseudo-anonymization scores and ratings (*see* illustration below), as already proposed by a scientific publication since 2021[562] . To sum up, online *anonymity is a* question of striking a balance between systematic contextualization of needs and existing levels of *pseudo-anonymity. In* the final analysis, the search for *anonymity* should not be outlawed, as it is what actually enables Internet users to choose *pseudo-anonymous* solutions that protect their privacy. The blockchain technologies and decentralized digital identity studied in a second part of this research will play a crucial role in recognizing a new era of digital privacy, in which *anonymity* will be possible for certain solutions, while *pseudo-anonymity* will remain commonplace for certain secondary attributes of the decentralized digital identity, the subject of this study.

strong enough, he reduced Patoshi's 10-minute block target to give others a better chance of mining a block". Whale Alert, "The Satoshi Fortune", 2022, Medium

[560] Contributors to bitcoin/bitcoin. August 30, 2009. GitHub. Retrieved October 14, 2022, from

[561] Witness the countless blockchain projects that exist and are headed by a foundation, a company or even an icon (reference to the Ethereum blockchain); *v, supra*, I, Title 1, 2.3.1.1.a

[562] KOLAIN Michael, GRAFENAUER Christian, EBERS Martin, "The anonymity assessment we propose in this paper will determine a set of two scores. The Objective Anonymity Score (OAS) determines the residual risk of (re)identification of a natural person according to objective statistical measures. It serves as a tool for measuring the properties [...] of a dataset processed by the IT system under evaluation, without taking into account additional information from other sources. The Subjective Anonymity Score (SAS) provides an indicator of the relative anonymity of the processing carried out by a controller or processor: it takes into account the cost and time required to successfully re-identify the data set in question, taking into account the controller's or processor's available manpower and capital", "Anonymity Assessment - A Universal Tool for Measuring Anonymity of Data Sets under the GDPR with a Special Focus on Smart Robotics", 2021, in *US Law and Tech Journal,* pending publication (forthcoming), accessed online on 20/12/2021.



1.3.1.1 From identity theft to the risk of widespread deception

Historically taking the form of the theft, fabrication or falsification of physical identity documents, the crime of identity theft has rapidly moved into the digital sphere. The multiple needs of people to access, identify and authenticate themselves online are paving the way for new, more sophisticated methods of remote identity theft. In 2019, 45,000 cases of identity theft were recorded in France[563] . Depending on the context of the identity theft, a number of offences may be considered, including but not limited to breach of confidentiality of correspondence[564] , invasion of privacy, collection of personal data by fraudulent means[565] , counterfeiting, etc.

[563] "Trois questions sur la nouvelle carte d'identité qui entre en vigueur lundi 2 août", in *Franceinfo*, published on August 2, 2021, consulted online
[564] Art. 226-15 of the French Penal Code (misappropriation, fraudulent use of private correspondence, even electronically).
[565] Art. 226-18 of the French Penal Code (collection of personal data by fraudulent, unfair or unlawful means).

and the fraudulent use of means of payment[566] or scams[567] . For legal institutions, another more specific form of usurpation is on the rise: behavioral fraud via identity loans[568] . In this respect, some administrations are combating identity lending, referred to by legal experts as "behavioral fraud", which is not yet covered by the eIDAS Regulation[569] , which is examined in the second part of this study. Behavioral fraud consists in borrowing a consenting person's identity in order to carry out one or more actions on his or her own behalf and in return for a fee. With the Covid-19 crisis and the introduction of the[570] health pass, this type of fraud has become particularly widespread. While the primary motivation for identity theft is to pretend to be someone else, individuals are the main victims, as are corporate entities (president fraud, swindling, phishing, domain name theft, etc.). In reality, it is not a person's identity that is usurped, but rather their rights. Their identity is not taken away, but rather duplicated in order to improperly acquire all or part of their rights[571] . Identity theft is defined by the LOPPSI 2 law[572] and in article 226-4-1 of the French Penal Code, which states that "it *is an offence to usurp the identity of a third party or to make use of one or more data of any kind enabling him* [a third party] to be *identified, with a view to disturbing his peace of mind or that of others, or to prejudice his honor or consideration* (...)"[573] . This is an offence punishable by one year's imprisonment and a €15,000 fine, a relatively dissuasive penalty given the serious and sometimes irremediable consequences for the victim. It is worth noting that the phrase "*one or more data of any kind enabling it to be identified" is* interpreted to include any identity attribute belonging to a person, including in the case of pseudo-anonymous identifiers, which is an encouraging prospect. The consequences of identity theft can be devastating*: "What's special about the Internet is that even if identity theft can be prosecuted under criminal law, the damage to image and reputation can be irreversible, given the impracticality of the right to b e forgotten. Only the right to dereferencing can be envisaged*"[574] . Victims of identity theft face numerous legal and administrative hurdles before they can hope to reintegrate their identity and enjoy their rights once more. As Pauline Elie, a doctoral student in law, explains: "*Victims of identity theft*

[566] Art. L163-3 (counterfeiting or falsifying a cheque) and L163-4 (manufacturing, holding, transferring or making available instruments or computer programs to commit offences) of the Monetary and Financial Code.
[567] Art. 313-1 of the French Penal Code (definition of fraud).
[568] This involves a person "lending" one or more elements of his or her civil identity to another person in order to obtain access to one or more rights. This relationship is generally monetized and illegal, and constitutes an offence of identity theft for the fraudster.
[569] See *infra*, II, Title 1, 2.1.1.1.
[570] ELIE Pauline, LANGLOIS-BERTHELOT Thibault, et al, "Le pass sanitaire au prisme de l'informatique, du droit et de la philosophie", Video workshop(s) and proceedings. 2021. *Les Temps Numériques*. Website available at the following address
[571] DESJARDINS Cécile, December 6, 2021, "La certification PVID permet de réduire le risque d'usurpation d'identité", in *Les Echos*, consulted online on 12/01/2022.
[572] Loi n° 2011-267 of March 14, 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (known as LOPPSI).
[573] Art. 226-4-1 Penal Code in the version in force since August 1er 2020, consulted online
[574] *Op. cit.* BENSOUSSAN Alain, Avocats, December 2021, "l'identité numérique 5.0", in *Lexing*, p.31.

It is extremely difficult for people who have lost their identity to re-establish their identity"[575] . For example, in the event of conviction for identity theft, it is extremely complex to remove the mentions corresponding to fraudulent acts that have been annulled[576] , until the enactment in 2022 of a proposed amendment to the law on the protection of identity "(...) the present article resolves this difficulty by requiring that, when an act is annulled by the judge on the basis of identity theft, it must be recorded in the register of births, marriages and deaths.) *the present article resolves this difficulty by requiring that, when a deed is annulled by a judge on the grounds of identity theft, the operative part of the judgment whose transcription is ordered in the civil status register must refer to the theft, which will make it possible, in future, to distinguish between the entries made in the margins of civil status registers, those which are the result of fraud and those which are not*"[577] . Today, certain certified verifications are already required as part of the creation of a digital identity by certain trust services under the eIDAS Regulation (electronic signature[578] , visible electronic seal[579]), or with the implementation of a repository for remote identity verification (PVID) providers[580] , which are examined in the second section of this study. Although the processes and guarantees of these trust services are effective, they are still being deployed relatively slowly and marginally in relation to the number of existing online services and the multiple identification needs and contexts of Internet users. So, although these services are essential for combating identity theft by legal entities and their online services, they are not yet able to combat identity theft by individuals on a massive scale. This is particularly true for the choice of storage methods for these digital identity attributes, which could make use of a decentralized identity, for example with P2P storage, which is explored further below, coupled with a blockchain. It would seem that decentralized digital identity can effectively combat digital identity theft, both upstream and downstream of digital identification needs, since it simply offers new verification and control mechanisms, directly or indirectly (*see* self-sovereign digital identity, studied below)[581] managed by users. The legal recognition accorded by the revision of the eIDAS Regulation[582] to private and hybrid blockchain registers, as well as to verifiable attestations[583] also studied later, reflects a

[575] ELIE Pauline, "Analyzing identity in law: how to protect and define a new territory in the dematerialized era?", *v*. Thesis in progress at EHESS, available at the following address

[576] "The rules governing the complete preservation of civil-status entries prohibit the pure and simple removal of entries corresponding to annulled acts. The operative part of the judgment annulling the record is entered in the margin without any other indication, which makes it impossible to distinguish between annulment due to usurpation and annulment for a reason specific to the person concerned", Senate. June 1, 2022. Proposition de loi relative à la protection de l'identité, in *sénat.fr*, consulted on 20/06/2022 and available at the following address

[577] *Ibid*.

[578] V*, supra*, I, Title 1, 2.3.1.1.b

[579] ANTS, *Le cachet électronique visible de la nouvelle carte d'identité*, available at the following address

[580] The aim of this standard is to highlight robust solutions, with two levels of guarantees: the
The "substantial" level, which offers the same reliability as face-to-face identity verification, and the "high" level, which achieves the level of reliability of issuing an identity document at the town hall, or from the gendarmerie. "Publication du référentiel d'exigences applicables aux prestataires de vérification d'identité à distance (PVID)", on *ANSSI*, online, accessed February 17, 2022.

[581] See *infra*, II, Title I, 1.4.

[582] See *infra*, II, Title 1, 2.1.1.1.

[583] See *infra*, II, Title 1, 1.3.1.2.

reaffirmed determination to combat the impersonalization of digital identities through new, reliable and sovereign tools, always at the service of citizens' identities.

1.4 Comparative geopolitics of personal data in Europe and the United States

Since the adoption of the Internet, European legislators have tended to model their regulations on those of the USA, despite a rather paradoxical[584] ideological divide between these two jurisdictions, which this section proposes to introduce with a view to understanding the necessary adaptations to be considered. It is proposed to move towards an overview of how these jurisdictions deal with the processing and protection of personal data, as blockchain technologies involve cross-border storage of encrypted data. The geopolitical history between these two sides of the Atlantic is likely to affect the legal frameworks applicable to crypto-assets, blockchain technology and digital identity 3.0. In the United States, personal data can, among other things, be commercialized, as it is considered the property of its holders and owners[585] . In Europe, the RGPD studied further, introduces specific legal protection for individuals with regard to the management of their personal data, the commercialization of which does not represent a possibility or even an opportunity, but rather a fundamental risk. Business secrecy or process secrecy does not fall within the scope of the RGPD (examined in the next chapter), unlike the law applicable in the United States, where all data can be marketed without distinction of origin (depending on whether it concerns natural or legal persons). On the other side of the Atlantic, infringement of this new monetizable Eldorado constitutes economic damage for the holder (whether a company or an individual). The presence of economic harm is not an essential prerequisite in European law for establishing fault in the processing of personal data, unlike practice in the United States, where the protection of individuals is less effective. This raises the question of the territoriality of the law applicable to the Internet: application of American law (federal or state) or of European regulations? The Court of Justice of the European Union (CJEU) had to rule on this issue in 2020 and concluded in a Schrems II ruling[586] , to which we will return, that US law is not compatible with European law and that the European RGPD finds application in matters of personal data protection[587] (the case of an Irish citizen in this instance). In practice, the authorities

---

[584] *Common law* deals with facts that give rise to legal rules, while *civil law* is largely based on statute law and regulations.
[585] Except in certain states (Utah, California, Colorado, Virginia) where the *California consumer privacy act (CCPA)* is in force. For more information, consult the following digital map (updated 07/04/2023).
[586] CJEU ruling of July 16, 2020, invalidating Decision No. 2016/1250, issued in the context of a preliminary question referred to the Court, concerning the adequacy of the protection provided by the EU-US Data Protection Shield, Aff. C-311/18, available at the following address, see also CJEU Press Release "Data Protection Commissioner / Maximillian Schrems and Facebook Ireland", no. 91/20 available at the following address
[587] *Ibid:* "The [...] GDPR provides that the transfer of such data to a third country may, in principle, only take place if the third country in question ensures an adequate level of protection for such data."

However, U.S. government agencies can access the personal data of European citizens to combat illegal, terrorist or money-laundering activities. The European Data Protection Regulations (RGPD and eIDAS, discussed below) regularly find themselves in conflict with various American regulations, including and non-limitatively for the most recent, the "Patriot Act"[588] of 2001, the "Foreign Intelligence Surveillance Act

- (FISA)"[589] of 2018, the "Cloud Act"[590] of 2018 or the "Executive Orders"[591] . However, these schemes are insufficiently monitored, and lack adequate remedies comparable to those provided by EU data protection law. These legal bases are those that allow the US government and its institutions - notably the National Security Agency (NSA), the FBI *and* the CIA - permanent access to the personal data of individuals. When it comes to digital data sovereignty within the European Union, the European Commission bears a significant share of the responsibility, having signed the *Safe Harbor* agreement in 2000[592] . This agreement provided for supposedly equivalent data protection rules, enabling the free flow of data between the USA and Europe. In fact, this legislative arrangement enabled the USA to collect data from European citizens for over a decade, while benefiting from a network effect and unrivalled experience in the Web 2.0 field. This situation propelled the United States to the rank of Internet leader. This situation gradually came to an end with the emergence of certain disturbing revelations, such as the Snowden affair[593] in 2013, followed by the referral of the case to the CJEU, which decided to overturn *Safe Harbor* in a ruling on October 6, 2015[594] . As a result, a new agreement was quickly adopted on July 8, 2016, the *Privacy Shield*[595] , which was also overturned by the *Schrems II* ruling on July 16, 2020[596] . This complexity in the European Commission's understanding and supervision of individuals' data led to a new political and legal positioning vis-à-vis the United States, based on the adoption of the RGPD, which came into force on May 25, 2018 after four years of negotiation (2012-2016)[597] . While the Commission

[588] The *Patriot Act*, which came into force on October 26, 2001 in the wake of the September 11 attacks, and has since been strengthened on several occasions.
[589] Committee on civil liberties, Justice and Home Affairs, "Background note on US legal instruments for access and electronic surveillance of EU citizens", in *Europa.eu*, available at
[590] The *Cloud Act* allows US intelligence services to access any foreign *cloud* provided by companies domiciled in the USA. Since *clouds* are provided all over the world, under the *Cloud* Act the USA can carry out searches without their customers' knowledge or authorization. *Compte rendu de la Commission de la défense nationale et des forces armées*, Assemblée nationale, hearing, in camera, of Mr Stéphane Bouillon, General Secretary for Defense and National Security, July 13, 2022, *v.* Compte rendu n° 5.
[591] BENZINA Samy, "Les executive orders du président des États-Unis comme outil alternatif de législation", in *Revue de droit politique*, Dalloz, 2018, hal-02900076
[592] Wikipedia contributors, "International Safe Harbor Privacy Principles". December 25, 2021, accessed April 4, 2022, at
[593] T.d.L, "Tout comprendre sur l'affaire Snowden", 2017, in *Leparisien.fr*. Accessed on April 4, 2022, at the following address
[594] CJEU ruling of October 6, 2015, Aff. C-362/14, decision given in the context of a reference for a preliminary ruling from the Court concerning the transmission by Facebook Ireland Ltd of Mr Schrems' personal data and their storage on servers located in the United States, accessed on October 17, 2022, at.
[595] CNIL: "Invalidation of the Privacy shield: the EDPS's first questions and answers", consulted on October 17, 2022, at the following address
[596] CJEU ruling of July 16, 2020, *op. cit.* available at the following address
[597] "The History of the General Data Protection Regulation", in *European Data Protection Supervisor*, consulted on October 20, 2022, at the following address

The European Commission is learning from its past mistakes (*Safe Harbour* and *Privacy Shield* were overturned by the CJEU), and it should be remembered that this period of reflection has enabled it to move from an ultra-liberal perception of data to a conservative and protective one for individuals. The Commission's aim is to create a European digital ecosystem, in which the rules applicable and enforced will be European, rather than bilateral and subject to the extra-territoriality of American law mentioned above. However, the case law of the CJEU may take several years to be transposed and applied by national control institutions (CNIL, AEPD in Spain, BFDI in Germany, etc.)[598] within the member states of the European Union. During these periods of political influence with legal effects, legislators are subject to strong pressure from the United States, and particularly from its major technology companies. Strict application of CJEU rulings by all member states would also mean constraining the activities of the US technology companies that founded the Internet (Microsoft, Google), which paradoxically all European citizens need on a daily basis. Geopolitics and law therefore seem unconditionally linked when it comes to the protection and patrimonialization of personal data (*see* below).

1.4.1 Territoriality of applicable law: between territories and conflicts of law

This section explores the massive transfer of personal data from the European Union to the USA, which raises numerous issues in terms of privacy, national security and economic competitiveness. Major technology companies (GAFAM/BHATX) use jurisdiction clauses in their general terms and conditions of use, for example, to impose their jurisdiction in the event of disputes. While some countries seek to maintain equivalent legal regimes for the protection of personal data following the example of the European RGPD, other countries tend to develop their own data protection rules, as illustrated by the United Kingdom since its exit from the European Union[599] . Blockchain technologies are, as we have seen, *pseudo-anonymous* and *decentralized in* nature, which presupposes that the participants (validating computers, developers, users) are spread across several countries under various jurisdictions. In a European case

[598] CNIL, "La protection des données dans le monde", *see* CNIL's interactive map of international data protection, at
[599] "Maintaining equivalence with European data protection laws [RGPD] may no longer be a priority for the UK as it moves towards a new pro-growth, pro-innovation regime - we may start to see some divergence in the coming years, and it will be important to keep abreast of new developments," translated from report in English published by The Law Society. Accessed online 12/01/2022, in *Blockchain: Legal and regulatory guidance* (No 2), p.144.

recently[600] , the holder of a crypto-asset portfolio opened with a Lithuanian company had summoned the latter before the Tribunal de Grande Instance (now TJ) of Montpellier for compensation after having been pirated of the sum of €300,000. The contract between them included a clause conferring jurisdiction on Lithuania. The Montpellier Court had dismissed the claim, but the Court of Appeal recognized the jurisdiction of the Montpellier Court on the grounds that the claimant was a consumer within the meaning of the Brussels I bis Regulation[601] . Territorial jurisdiction remains a major issue in the conclusion of European and international contracts, even though Europe now has numerous regulatory provisions, discussed below, enabling it to avoid the pitfalls imposed by third countries outside Europe, which are particularly present in new technologies and their blockchain applications.

Chapter 2: Law meets blockchain technology: issues and chronology

2.1 - Decentralization for the common good and a new digital society

The various possible uses of blockchain technologies have an impact on several branches of law. On the one hand, players in the crypto-asset ecosystem, such as developers and technophiles, argue that 3.0 computer programs have a "*code is law*" normative scope[602] and on the other hand, a majority of jurists argue the opposite "*law is code*"[603] , sometimes without taking into account the potential of decentralized programs often due to a lack of knowledge. In practice, it seems that each of these expressions influences and contributes to making the other's law, until a point of equilibrium is reached or accepted, generally under the impetus of the market and the legislator. Decentralization can be seen as the computerized and social redistribution of roles to as many different entities as possible. The aim is for an online service no longer to rely on one or more trusted third parties, but on a multitude of agnostic entities who trust each other thanks to a geographically distributed, transparent and secure digital infrastructure, where participants are, as we have seen, *pseudo-anonymous* (public blockchains). In theory, decentralization is always possible when it is conceived as the de-escalation of an existing, centralizing power. It should be seen as the recentralization of autonomy

[600] CA de Montpellier, Civ. 2ème ch., October 21, 2021, N°RG 21/00224, "L'utilisateur d'une plateforme de services de cryptomonnaies est un consommateur au sens du Règlement Bruxelles I bis", in *Actualité Droit Propriété Intellectuelle Technologie de l'information Innovation* - Cabinet Simon et Associés Avocats, "La Cour s'est prononcée sur la compétence territoriale des juridictions montpelliéraine dans une affaire de piratage d'un portefeuille de cryptomonnaies ayant donné lieu à un vol de l'équivalent de 300.000 euros". Consulted at the following address

[601] Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of December 12, 2012, on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters.

[602] LESSIG Laurence, internationally renowned American jurist, "Code Is Law - On Liberty in Cyberspace", January 2000, in *Harvard Magazine*, available at

[603] In French, this expression could be translated as "The law is computer code".

previously dependent on one or a few third parties, to a new form of independence, more autonomous and managed by a multitude of new decentralized technologies. In other words, decentralization implies a shift in political and social control, from one or more centralizing entities to crowds of people belonging to a single online community. However, decentralization is generally utopian if it is only understood from a computing point of view, i.e. when no research or need for trusted third parties is involved, as is the case with the Bitcoin protocol, which involves few trusted third parties for its operation[604] . Far from this radical technical standard, rather extreme in the eyes of neophytes, and facing numerous contradictions, it is nevertheless admitted in this research that computer decentralization can bring certain benefits to the digital society. However, as Jean Lassègue and Antoine Garapon point out, "*digital technology is leading the world towards ever greater radicalism [...] a rule that no longer needs words, and which can therefore no longer be interpreted*"[605] . One of the basic tenets of this study is that society will always need centralization and intrinsic trust to thrive. Blockchain technologies make it possible to test hypotheses based on certain elements that are currently centralized and that it is possible to imagine operating in a partially decentralized way. To fully understand the nuances and degrees of IT decentralization that exist for each blockchain technology, several non-exhaustive considerations can be presented[606] :

(i) The economic mechanisms of each blockchain (*Proof of Work*, *Proof of Stake* and *Proof of Authority*)[607] studied below, are designed to motivate and encourage each user of the network to contribute to its operation and validation in a more or less decentralized way. It turns out that the greater the economic incentive, the more users have an interest in getting involved in the network, creating a network effect[608] attracting communities of developers and then Internet users.

(ii) When a blockchain protocol offers greater transparency and accessibility to its source code and software code, it reinforces the trust that users place in it.

---

[604] V. Appendix 3, Focus 1 to 6.
[605] *Op. cit*. LASSEGUE Jean, GARAPON Antoine, "Justice digitale", p.158.
[606] SRINIVASAN Balaji, "Quantifying Decentralization", July 28, 2017. Some specialists have been proposing since 2017 six different subsystems to measure the decentralization of a blockchain (mainly applicable to the *proof-of-work mechanism*): its mining, code base, developer community, exchanges and transactions, nodes and ownership of blockchain addresses, in *news.earn.com,* available online
[607] V. Appendix 6, Focus 1 to 3.
[608] Term popularized by Robert Metcalfe with his theory of the *network effect* or *Metcalfe's law*.

(iii) The size of the developer community is a key element in keeping blockchain up-to-date and well-equipped to meet computing challenges near at hand, such as the congestion of public blockchains, or further afield, such as the threat of quantum supremacy.

(iv) In principle, an older blockchain with a large number of exchanges and transactions carried out by its users is considered more resilient, decentralized and likely to meet the aforementioned criteria.

(v) The number of computers (nodes)[609] dedicated to a blockchain technology is an important factor, because the more computers interconnected on said blockchain, the more immutable the data is and the more it is copied on a large number of computers.

(vi) The distribution of wealth within a blockchain technology depends on the economic mechanisms and incentives put in place by its developer community. In this respect, it is important to avoid the financial centralization of funds in crypto-assets on a small number of blockchain addresses[610] , to guarantee a fair distribution of funds among users and ensure the economic sustainability of the blockchain in question.

Blockchain technologies can take different forms, more or less robust and proven, depending on the IT and socio-economic choices of computer networks. However, their common objective is to offer a new, decentralized 3.0 version of the digital universe, more transparent and secure for Internet users. Although blockchain technologies are sometimes synonymous with disempowerment for certain jurists, for whom the crypto-economy is merely a means of evading the rules of law, this research sees blockchain technologies as fundamentally reliable and intrinsically trustworthy. For this vision to prevail, we must seek to frame these new technologies and their applications with moderation, rigor and pragmatism. We need to understand decentralization in order to tame it better, and not necessarily seek to regulate or contain it. In fact, to frame and contain this desire for decentralization too soon would be to limit any chance of Internet users or States interested in reasserting their online sovereignty reclaiming the digital sphere. Decentralization is beneficial if it remains at least under the control of a state governed by the rule of law. This requires

[609] V. Appendix 3, Focus 2 and 3.

[610] For example, on the Bitcoin blockchain, it is possible to publicly consult the addresses that contain the most bitcoins to date. These figures should be viewed with a certain amount of hindsight, as many of the bitcoins on these addresses are inaccessible to their owners, who have lost access to them (private cryptographic keys). For example, in the early days of Bitcoin, around 907 bitcoins were spent by *Satoshi Nakamoto* and 1,125,150 bitcoins mined (equivalent to over $26 billion as at 12/08/2022). These funds are most likely inaccessible and blocked forever due to the loss of the associated *private keys* (contrary to a false but widely held view by some media that Bitcoin is a *Ponzi scheme* since *Satoshi Nakamoto is* single-handedly centralizing this large amount of bitcoins), v. "Top 100 Richest Bitcoin Addresses and Bitcoin distribution", June 21, 2022, in BitInfoCharts, accessed June 21, 2022, at. V. Appendix 3 & 6

that it can design its own IT equipment[611] , software, applications and languages. Otherwise, even decentralized control of the digital identity ecosystem and value chain could be compromised by third parties with often conflicting (geo)political objectives. The State must ensure its own know-how and nurture talent. Without these cumulative elements, blockchain technologies and decentralized digital identities remain fallible and subject to dependencies and risks of attack[612] . For the majority of use cases and business applications, it is assumed that only public authorities in partnership with specialized players in the digital ecosystem could have the capacity to achieve and deliver a fair and satisfactory degree of IT and social decentralization. A decentralized regal identity must be based on a contract and a social negotiation framed by law, i.e. it must be understood and consented to by all citizens. If the state were able to design its own hardware, software and applications, this would enable it to maintain a degree of technical control over the digital ecosystem, even if digital identity were decentralized. Without this control, third parties could compromise the security of the digital identity ecosystem and value chain, with objectives that often run counter to those of the State.

To conclude at this point, decentralized digital identity proposes a redefinition of the concept of digital identity. With a decentralized digital identity, every individual knows and owns a cartography, a dashboard of his or her digital identity attributes. This new personal sovereignty does not mean, however, that individuals will systematically issue their own identity credentials on their own, but rather that they will be able to control certain functionalities in the use and sharing of their personal data. The use of cryptographic proofs will enable every Internet user to receive, manage, store and share their identity attributes online in a verifiable way, thanks to cryptography, thus enabling the actors with whom they share them to verify them. This makes this new technology accessible, transparent and open, a tool at the service of the common good. This research considers that society must understand and appropriate this new technological perspective without delay.

---

[611] This refers to a state's sovereignty over its "*middleware*", i.e. *software* and hardwares.
"Taiwan] holds about two-thirds of the world's production capacity for wafers, the single-crystal silicon wafers that form the basis of all electronic chips", v. also "to conquer or submit".
réflexion autour des contraintes d'une réunification "forcée" de Taïwan à la République Populaire de Chine", in *Theatrum Belli*, published November 5, 2021, accessed online November 10, 2021.

[612] To counter this dependence, the European Commission is proposing a law on electronic chips to counter the shortage of semiconductors and strengthen the EU's technological leadership, in *Digital sovereignty*, European Commission, online, accessed March 4, 2022.

2.1.2 Blockchain, a limited alternative to traditional institutions

For French academic and jurist Alain Supiot, Professor Emeritus at the Collège de France, institutions are indispensable to a society: "*Institutions are the frameworks within which human freedom can be expressed*"[613] . In principle, institutions are governed by rules established democratically and supervised by a state. While seemingly far removed from these principles and conventions, decentralized systems rely on new mathematical and cryptographic rules to form a new type of online social organization. A structural distinction thus emerges between these two environments, as the notion of institution in one or other of these ecosystems does not refer to the same definitions or realities. In the 3.0 universe, an institution can be socially recognized and legally non-compliant with positive law. Some public blockchains (Bitcoin, Ethereum)[614] challenge the power of certain public institutions, particularly in monetary terms[615] . They are tending towards a real degree of IT and social decentralization, i.e. they hold an unprecedented power to overturn the role of established monetary institutions. Thus, it is legitimate to ask certain questions regarding the impact of blockchain technologies in a state governed by the rule of law: to what extent can a blockchain technology challenge a state governed by the rule of law? Can it establish itself as a credible digital alternative to public and political institutions? Could certain blockchains replace our current social and institutional models? However, it seems that most of the physical impacts and effects of blockchains are limited for the time being. Indeed, if blockchain technologies with their IT applications do not systematically and rapidly integrate certain legal, institutional and social requirements, their adoption will be slower. The economic incentive mechanisms that enable public blockchains to function appear to run counter to certain social and legal principles, such as the principles of equality and data transparency, or the fight against online anonymity. In the long term, however, the innovative potential of public blockchains should not be underestimated, as they could host a host of social applications that are still in their infancy. In terms of our political and legal institutions, public blockchains ultimately suffer from several limitations due to their complex articulation and modes of governance. Governments and regulators are better equipped to monitor and regulate traditional institutions, while blockchains remain unexplored in regulatory terms. Ultimately, blockchain technologies are a promising alternative to traditional institutions, but they still remain limited in their potential and ability to completely replace existing systems. Only certain areas appear to be directly confronted with a high degree of IT decentralization in the short to medium term.

---

[613] SUPIOT Alain, Professor emeritus at the Collège de France, "The problem is to know how to put our new tools at our service instead of identifying with them and trying to program us", "compte-rendu d'un échange", CNNum, September 24, 2021, in *cnnumerique.fr*, consulted on 24/09/2021 at the following address also available at the following address

[614] V. Appendix 6, Focus 2.

[615] See *infra*, II, Title 2, 2.4

2.1.3 Introduction to the concept of the degree of IT decentralization

In domestic law, the term "*decentralization*" is evoked by Article 1er of the Constitution of October 4, 1958, which states that the organization of the French Republic and its territorial communities is decentralized[616] . In IT, and for the purposes of this study, this term takes on a completely different meaning[617] , that of disintermediation and/or geographical dissemination of computers, i.e. the ability to dispense with significant intermediaries for the design and operation of IT solutions. For Pierre Person, a former member of parliament and legal expert, "*the level of decentralization therefore appears to be a complex construct whose exhaustiveness cannot simply be summed up in a few lines*"[618] . In June 2018, the U.S. Securities and *Exchange Commission (SEC*) introduced the concept of sufficient IT decentralization[619] , a notion which inspires the concept of degree of decentralization introduced below. This technical principle states that a blockchain network is only truly decentralized when no single entity has the ability to control it. In this respect, Bitcoin[620] seems particularly decentralized, as a single entity cannot restrict its users' ability to use it freely. The open, public Bitcoin blockchain is therefore at the highest level of decentralization compared to other blockchains, so the terms "decentralized" or "decentralization" should be epistemologically reserved and circumscribed to this (truly) decentralized registry[621] . In reality, many Web 3.0 players use these terms for situations and levels of low or relative IT decentralization, which generates widespread confusion in the minds of the Web 3.0 target audience. In 2017, the Nakamoto coefficient (from the aforementioned Satoshi Nakamoto) was described for the first time by the former CTO of the American company Coinbase, Balaji Srinivasan[622] . This coefficient proposes a measure for the decentralization of a blockchain and represents the minimum number of actors and criteria required to disrupt such a network. The higher this coefficient is for a blockchain technology, the more decentralized it is, i.e. the more resilient it is to computer attacks[623] . Since 2017, this tool has confirmed that

---

[616] Full text of the current Constitution of October 4, 1958, *v*. Conseil constitutionnel, available at

[617] GOUJON Pierre, mathematician, "Le triomphe de la décentralisation", in *Universalis.fr*, consulted at the following address

[618] PIERSON Pierre, "Monnaies, banques et finance: vers une nouvelle ère crypto, un enjeu de souveraineté et de compétitivité économique, financière et monétaire", in *Rapport de l'Assemblée Nationale*, 2022, p.32.

[619] HINMAN William, "Digital asset transactions: when howey met gary (plastic)", 2018, free translation from English, for what is sufficient decentralization "If the network on which the token or coin is to operate is sufficiently decentralized - where buyers would no longer reasonably expect a person or group to perform the essential management or business efforts - the assets may not represent an investment contract." In other words, if a protocol and network is not sufficiently decentralized, the value of the associated crypto-asset may be derived from the efforts of a centralized team - a person or group of people who, depending on the audience, coordinate to increase its value. Conversely, if the protocol is sufficiently decentralized, the value of the crypto-asset is not derived from what the public believes to be the efforts of a centralized team. Available at

[620] V. Appendix 3.

[621] V. Appendix 7.

[622] SRINIVASAN Balaji, "Quantifying Decentralization", 2017, *op. cit.*

[623] Bitcoin has the highest Nakamoto coefficient. Its measurements are significantly higher than for most other blockchains. This makes Bitcoin one of the most decentralized blockchains. For example, Bitcoin has 14,409 validators and a *Nakamoto score* of 7,349, while most blockchains score below 15. PLATIS Mike, SANDERFORD Bergen, "Nakamoto Coefficient", 2022, in *CrossTower*. Available online

only the Bitcoin blockchain is decentralized and resilient. Indeed, the greater the number of[624] nodes on a blockchain, the more decentralized and immutable its data. Conversely, and still from an IT point of view, if blockchain technology is not very decentralized, i.e. with a limited number of nodes (*see* Appendices 3 and 6), the term "distributed" seems more appropriate than "decentralized". In fact, these two terms are currently used interchangeably and equivalently within Web 3.0, ignoring these gradual yet fundamental distinctions. Reaffirming the concept of a degree of decentralization makes it possible to refine the theoretical contours of blockchain technologies to better distinguish between those that are open, closed or hybrid. This scale of decentralization is also essential if lawyers are to be able to grasp and qualify each 3.0 solution and its legal implications with precision. Furthermore, in the light of Appendix 7 of this research, it is essential to distinguish between the aforementioned concept of IT decentralization and that of social decentralization, too often confused (see Appendix 7). The former refers to the ability of an IT system to operate autonomously, i.e. without depending on other IT systems. The second is broader and concerns social independence in human interaction, which is considered utopian given that Man is intrinsically a social being, as explained in the previous sections. Attempts at social decentralization are thus paradoxically opposed to any attempt at IT decentralization, since trust in others is essential in human interactions, even when they are digitized. For example, the Bitcoin blockchain may be particularly decentralized from an IT point of view, but its social ecosystem remains centralized by private companies and many of their employee-developers. Although Bitcoin users believe they are using applications that are decentralized and incensurable, their social and legal components are still largely centralized. This is particularly true for the "*Lightning Network - LN*"[625] studied in Appendix 3, which is a partially decentralized IT protocol, as it is attached to the Bitcoin blockchain, although it suffers from social and IT centralization due to its young age (2017). However, the question arises as to whether this quest for decentralization is really necessary, and in what situations? The answer is affirmative for public blockchains, which, for example, aim to offer cryptocurrency for the common good, particularly in countries where monetary or political instability is rife. On the other hand, this is not necessarily the case for private and hybrid blockchain technologies, which are already being used, and rightly so, to manage people's digital identities.

[624] V. Appendix 6, Focus 1 and 3.
[625] V. Appendix 3, Focus 4.

2.2 Legal issues raised by blockchain

For several years now, blockchain technologies have been raising a variety of legal questions, to which legislators are attempting to respond in heterogeneous but sometimes contradictory ways. The major challenge lies in the legislator's ability to develop appropriate and coherent legal rules for the market, without slowing down the life cycle and adoption of the third-generation technologies studied in this thesis. The difficulty is compounded by the cross-border and universal nature of the transmission of blockchain technologies, defying the traditional notion of space and territory. This raises the question of whether the law should adapt to blockchain technologies, or whether they should conform to existing legal rules. We also need to consider the potential impact of each type of blockchain on the law. The protection of personal data is a major challenge, given that blockchain technologies can enable data to be stored directly or indirectly, permanently and transparently, which can compromise the confidentiality of personal data. Industrial, literary and artistic property is also a major issue, as it can be difficult to determine who owns the rights attached to works, innovations or creations linked to a blockchain. The regulation of financial transactions is another key issue, as blockchain technologies enable financial exchanges without the intermediary of traditional banks. Finally, the responsibility of the players involved in the blockchain ecosystem must be considered in the same way as its compliance with national and international laws and regulations, which remain an important issue in guaranteeing the compliant, responsible and ethical use of any blockchain. 3.0 technologies, with their decentralized algorithms and applications, smart contracts, DAOs and decentralized identity standards[626] , differ from the centralized algorithms studied earlier. Unlike the latter, which are complex to regulate and audit due to their closed source codes[627] , 3.0 technologies benefit from being in a position to be audited and considered more transparent and secure. However, despite the supposed transparency of these decentralized technologies, their legal framework is also proving complex, especially where public blockchains are concerned. Depending on whether a business chooses a public, private or hybrid blockchain for its needs and/or services, the legal consequences are not neutral, particularly with regard to applicable law, competent jurisdictions, responsibilities and the rights and obligations of each stakeholder[628] . The table below provides a snapshot of the legal implications of public, private or hybrid blockchains for their users.

[626] See *below*, II, Title I, Chap. 1
[627] JEAN Aurélie, "Les algorithmes font-elles la loi?", "[...] it is impossible to regulate an algorithm for the simple reason that it is impossible to evaluate it fully", *op. cit.* Reading position in the book: 23%.
[628] BOURDAIS Gaëtan, "DSA : quelle responsabilité pour les fournisseurs de service intermédiaires ? (2/7)", in *Shift-avocats*, available at

Branches of law affected[629]	**Public blockchain(s)**	**Private blockchain(s)**	**Hybrid blockchain(s)**
Protection of personal data (RGPD)	□ or ~	□	□
Protecting the fundamental freedoms of Internet users	□	□	□
Compliance with the law of obligations	~	□	□
Respect for intellectual property	~	□	~ or □
Compliance with consumer law	~	□	□
Compliance with banking, tax and financial law	~ or □	~ or □	~ or □
Identification of parties	~	□	□
Key legal issues	*Which court has jurisdiction?* *Who has legal personality?* *Which law applies?* *Who is liable for damages* *(Network nodes, developers, service providers)?*	*Which court has jurisdiction?* *Who has legal personality?* *Which law applies?* *Who is liable for damages* *(Network nodes, developers, service providers)?*	*Which court has jurisdiction?* *Who has legal personality?* *Which law applies?* *Who is liable for damages* *(Network nodes, developers, service providers)?*

[629] See also Appendix 12.

In 2022, although the number of disputes relating to open and public blockchains is steadily increasing due to their gradual adoption by Internet users and businesses (for example, bitcoin-related disputes[630]), many of the previous questions remain unanswered or uncertain. While the number of such disputes today remains marginal compared to other sectors, it is likely that in the future the courts will be forced to decide disputes according to each category of blockchain involved. Public blockchains complicate the search for liability, not least because of the pseudo-anonymity mentioned in the previous chapter. Indeed, each interaction is potentially spread across numerous computers, geographically distributed around the world, whose owners may be difficult to identify. This complexity of digital identification can become a source of difficulty, particularly when it comes to applying complex legal decisions (tracing perpetrators, responsibilities, damages suffered). In fact, each transaction is potentially distributed between numerous computers located all over the world and belonging to owners who, in some cases, are impossible to identify. The management of personal data is a particularly sensitive issue for any public blockchain, on which it is in principle forbidden to publish or administer personal data that has not been encrypted by pseudo-anonymization mechanisms. Some threats are real, such as the publication and deliberate exposure[631] of personal data, or the theft and loss of cryptographic keys. These few examples can lead to serious violations of people's privacy, sometimes by vitiating their digital consents, which decentralized identity proposes to reinforce.

Private and hybrid blockchains, on the other hand, offer a more malleable technical infrastructure, enabling compliance by design. Governance represents the technical as well as the legal foundation within which it is possible to know who is in charge and who controls the blockchain, who has access to it and how, as well as where each node is located (see Appendices 3 and 6). In short, a closed blockchain ensures the identification of the technical managers and, where applicable, their associated responsibilities. As a result, it is easier to determine the applicable laws from the outset, and to identify the relevant jurisdictions in the event of a dispute. For a user, the dilemma is whether to trust a blockchain controlled by computer programs governed by a community of Internet users (open blockchains), or a blockchain controlled by computer code framed by clearly identified managers and laws (closed blockchains). Answering this dilemma would involve understanding the needs of the society likely to require both systems. Finally, knowing the category of blockchain concerned would make it possible, for example, to give legal guidance to the competent jurisdictions, to

[630] PAPPERS, "Search for court decisions - Pappersjustice". Retrieved October 19, 2022, from
[631] At the beginning of 2023, a new feature will enable any Internet user to publish information of any kind (photos, videos, codes, etc.) on the Bitcoin blockchain in an immutable way. Personal information has already been published and injected directly into Bitcoin blocks. For further information, visit the following site

know the potential legal effects, such as a place to store, process and transfer data, before the exact qualification of said decentralized network. Blockchain technologies do not a priori create a legal vacuum (with the possible exception of Bitcoin), as the Internet did when it was created, but rather legal uncertainties, notably through conflicts of law and difficulties of interpretation and application.

2.3 The legal status of blockchain and crypto-assets in domestic law

The first legal recognition of blockchain came in 2016 with the legal recognition of the "Dispositif d'Enregistrement Électronique Partagé - DEEP"[632] , better known to the general public by its English-language name of "*blockchain technology*". The Commission[633] d'enrichissement de la langue française has published a list of terms and definitions (digital assets, smart contracts, cyber tokens, etc.) applicable to blockchain technologies and their applications, without forgetting at the same time to recall the use of the French language for certain situations[634] . This French normative and linguistic recognition testifies to the interest in and gradual adoption of these new technologies, which are revolutionizing the way digital information is shared, both technically and conceptually. France is the second European country, after Estonia[635] , to have adopted a legal framework dedicated to blockchain technologies with the PACTE law of May 22, 2019, which notably introduced a definition of the *digital token*, initially undefined in the Monetary and Financial Code (CMF), translated from the English "*digital token*", by "*any intangible asset representing, in digital form, one or more rights that can be issued, registered, retained or transferred by means of a shared electronic recording device* [DEEP] *enabling the owner of said asset to be identified, directly or indirectly*"[636] . It should be remembered that the legal status of the *token* mentioned below depends on its nature, i.e. if it is considered a digital asset, it is subject to the provisions of the CMF,

[632] Art. L. 223-12 et L. 223-13 du CMF, *v.* Ordonnance n°2016-520 du 28 avril 2016 relative aux bons de caisse, prise en application de la loi Macron du 6 août 2015 pour la croissance, l'activité et l'égalité des chances, which gives blockchain technology its first legal recognition, *v.* also, "La France entérine l'usage de la blockchain pour certains titres financiers et confirme son avance législative à l'échelle internationale", in *Actualités & Publications*, Gide Loyrette Nouel, cabinets avocats, January 7, 2019, available online

[633] Avis et communication, JOEA n°0013 du 15 janvier 2021, Commission d'enrichissement de la langue française, v. Vocabulaire des actifs numériques

[634] Art. 3 and 4 of the Toubon Law no. 94-665 of August 4, 1994 on the use of the French language: "all inscriptions or announcements affixed or made on the public highway, in a place open to the public or in a means of public transport and intended to inform the public must be in French when they are affixed or made by legal entities governed by public law or private entities carrying out a public service mission. Only legal entities governed by public law are obliged to use these official translations.

[635] PICRON Antoine, "L'Estonie : modèle d'un état plateforme e-gouverné", in *Institut Sapiens*, "D'abord à partir de 2008, les pouvoirs publics estoniens ont progressivement intégré la blockchain au sein des administrations", p.31, available online. V. *supra,* I, Title 1, 2.2.2.1.c

[636] Art L.552-2 du CMF, *v.* CARRIER Marine, lawyer, "Ce que MiCA va changer pour les prestataires de services sur crypto-actifs (PSAN/CASP)", in *Village de la Justice*, October 17, 2022, available at

but if it is considered to be a financial security[637] then it is subject to the common characteristics of a financial security, i.e. it is created by issuance, materialized by an entry in an account or an entry in a blockchain, negotiable by account-to-account transfer, and its possession is equivalent to a security. Its legal status is therefore important, and if it is considered a financial security, it is subject to much stricter rules when it is issued and traded.

It may be briefly recalled the genesis of the main texts intervened in domestic law from 2016 to 2022 for the benefit of blockchain technologies:

- Ordinance no. 2016-520 of April 28, 2016[638] on savings bonds introduces a new section 2 into the CMF relating to minibonds, and provides for their issuance and sale via a "mini-bond". blockchain. It should be noted that no distinction is made between open and closed blockchains.
- Law n°2016-1691 of December 9, 2016, known as Sapin 2[639] , empowering the government to take measures concerning the law applicable to financial securities and securities in order to enable their representation and transmission by means of a blockchain.
- Order no. 2017-1674 of December 8, 2017[640] on the use of a DEEP for the representation and transmission of financial securities providing for the representation and transmission of financial securities by means of a blockchain.
- The Decree n°2018-1226 of December 24, 2018[641] on the use of a DEEP for the representation and transmission of financial securities and for the issue and sale of minibons, specifying the conditions of application of the aforementioned orders of April 28, 2016 and December 8, 2017.
- Law n°19-486 of May 22, 2019 on the growth and transformation of businesses, known as the PACTE law[642] , governing ICOs[643] and digital assets within the meaning of Article L. 54-10-1 of the CMF, or a token within the meaning of Article L. 552-2 of the same code. This is the recognition of the registration of ownership of an asset on a blockchain.
- Decree no. 2019-1213 of November 21, 2019[644] on asset servicing providers Title IV of Book V of the CMF has been supplemented by a new chapter X, "Prestataire sur actifs numériques" (PSAN), incorporating the concept of DEEP. It should be noted that the French regime for PSANs, which are subject to mandatory registration with the AMF or to optional approval, is not yet in force.

[637] Art. L.211-1 of the CMF.
[638] JORF n°0101 of April 29, 2016.
[639] JORF n°0287 of December 10, 2016.
[640] JORF n°0287 of December 9, 2017.
[641] JORF n°0298 of December 26, 2018.
[642] JORF n°0119 of May 23, 2019.
[643] BOUILLET-CORDONNIER Ghislaine, et al. " La finance numérique, aspects juridiques et fiscaux du crowdfunding et des cryptoactifs", Titre I, chap. 2, pp.135-143, Cabinet Albatross Legal, 2021, *see* also, "Tour d'horizon du droit financier suisse, crowdfunding - ICO-STO", *op. cit.* ⟨hal-03282220⟩.

[644] JORF n°0271 of November 22, 2019.

is regularly called into question by many players in this ecosystem (lawyers, companies, associations) for a variety of reasons[645] .

- Ordinance no. 2020-1544 of December 9, 2020[646] strengthening the framework for the fight against money laundering and terrorist financing applicable to digital assets.
- The proposed European Regulation on the Crypto-Asset Market ("*Markets in Crypto- Assets"*) of the Parliament and Council, known as MiCA, published on October 5, 2022, with the ambition of creating a harmonized legal framework within the EU for activities involving crypto-assets. This Regulation is discussed in detail later in this chapter.

The foregoing observations lead us to consider that the French legislator has opted for a "European legislators have opted for "*regulation by the software infrastructure*", which we'll look at later, but also "regulation *by the market",* albeit inspired by the texts of the French legislator.

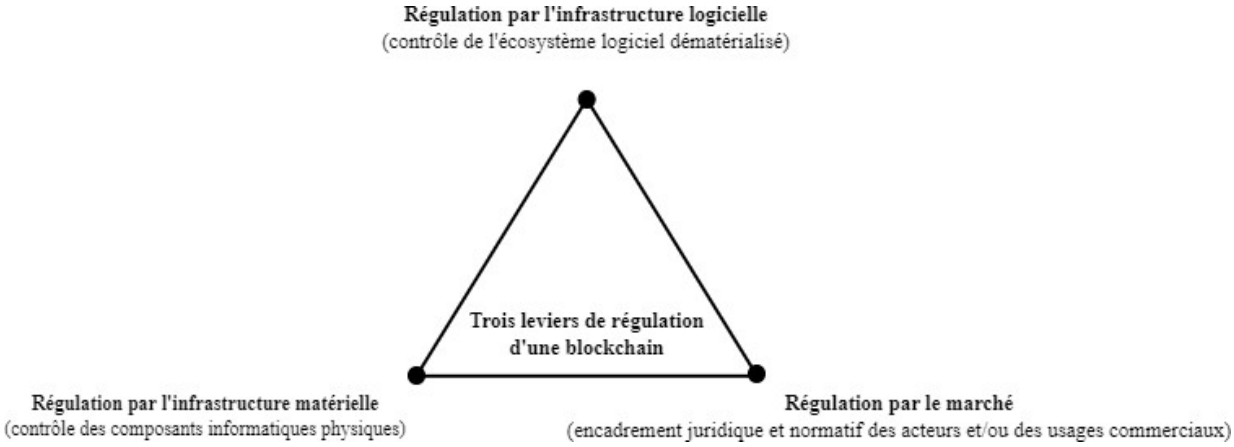


Diagram inspired by the remarks in Chapter 11: Blockchain & regulation 1, in "Blockchain and the Law", De FILIPPI Primavera.

[645] While the NSP regime has the merit of acting as a regulatory *"sandbox" at* EU level, it is often called into question because of its high cost (between €35,000 and €150,000 to obtain this registration via a law firm). What's more, this registration does not improve respect for the *right to an account* for PSANs (whose bank accounts are regularly closed without justification). Finally, this status does not prevent foreign players from offering their services to French customers under the principle and exception of "reverse solicitation" or "provision of services on the sole initiative of the customer" as provided for in the MiFID 2 Directive (*reverse solicitation* is in our case the name given to the circumstances in which a potential customer approaches, supposedly on his or her own initiative, a foreign crypto-asset trading platform). This request must not, in principle, be in response to advertising or marketing of any kind on the part of the exchange platform (which is often not the case, as these foreign platforms have been soliciting French internet users since 2016).

[646] JORF n°0298 of December 10, 2020.

Ultimately, despite the pioneering and not inconsiderable efforts of the French legislator to qualify and provide a legal framework for crypto-assets, a number of difficulties remain. A first step towards resolving them could be to recognize them by lifting persistent banking and institutional taboos - and lobbies - and at the same time promote a decompartmentalization of consciousness through a subtle combination of education, innovation and collaboration. This would make it possible to legislate in favor of new legal and economic approaches, given today's particularly rich technological context, in active collaboration with major public, financial and governmental institutions.

2.4 Blockchain and data protection (RGPD) in the EU

On March 9, 1993, mathematician, computer engineer and Cypherpunks Eric Hugues considered that "*a private matter is something you don't want the whole world to know, but a secret matter is something you don't want anyone to know. Privacy is the power to reveal what you want to whom you want*"[647] . Several decades later, the ecosystems of crypto-assets and blockchain technologies are still inspired by the ideas published by Eric Hugues in his "*Cypherpunk Manifesto*"[648] . For several years now, some of these principles have appeared in line with certain legal texts and rules dedicated to the protection of personal data. The notion of data originated in the French Data Protection Act of January 6, 1978[649] . In 2004, article 2, 2ème §, of a new version of the law, now repealed to be amended, stated that "*personal data is any information relating to a natural person who is identified or can be identified, directly or indirectly, by reference to an identification number or to one or more elements specific to him or her. To determine whether a person is identifiable, it is necessary to consider all the means by which he or she can be identified* (...)"[650] . This development suggests a particular attachment to the protection of personal data and identifiers, with reference to the online pseudo-anonymity mentioned above. Later, Regulation (EU) 2016/679 of the European Parliament and of the Council on data protection, known as the RGPD[651] , came into force on May 25, 2018 and transposed the fundamental principles of the French legislator's aforementioned definition of data protection

[647] HUGHES Eric, "A Cypherpunk's Manifesto", available at
[648] Wikipedia contributors, "Cypherpunk", 2023, available at
[649] Art. 4 of the law introduced the notion of "nominative data" in 1978, Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, "information is deemed nominative within the meaning of the present law if it enables, in any form whatsoever, directly or indirectly, the identification of the natural persons to whom it applies, whether the processing is carried out by a natural person or by a legal entity", available at the following address
[650] *Ibid*. Version in force from August 07, 2004 to May 25, 2018.
[651] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (RGPD), entered into force on 25 May 2018, accessed online on 10 November 2021.

personal data. Article 4 of the Regulation lists the elements constituting the identity of a targeted natural person, with a view to ensuring greater protection of his or her data: "*any information relating to an identified or identifiable natural person* (...)*; an 'identifiable natural person' is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or to one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity*". In addition to this legal definition of data, consider the more general IT definition, which defines it as "*all information that describes quantitatively or qualitatively an entity, an individual, a situation, a phenomenon or a legal person".*

"[652] . Before examining in detail the legal consequences of the RGPD applicable to blockchain technologies and the decentralized digital identity (IND) studied below, it seems wise to introduce the following table:

[652] JEAN aurélie, "Les algorithmes font-ils la loi?", in *Humensis*, *op. cit.* reading position in the book: 16%.

Who is affected by the RGPD?	What data is covered by the RGPD?	What rights do people have?	What obligations do organizations have? ?	How do you prove compliance? What are the penalties?
All organizations processing the personal data of individuals administrations, public institutions, associations, companies and their subcontractors.	Any information relating to an identified identified or identifiable or identifiable individual: surname, first name postal address, geolocation, e-mail address (personal or business) or professional), address IP ADDRESS, cookies from navigation, personal identification number (CNI, social security card, etc.).	The protection of individual rights is strengthened. Individuals must be informed concise, understandable and easily accessible on use of the data collected. They must give their consent for this treatment and can object. The aim is to give to people the control of data about them.	Obligation to implement all necessary technical and and organizational measures appropriate à their activity for protection protection of personal data throughout of development process for their products or services.	Several solutions are available solutions: Inform individuals when of collection of data on the purposes and duration of data storage, as well as their rights (see below); Gather evidence of their consents ; Notify CNIL of any security breach in its system at processing and to inform the persons concerned as soon as possible in the event of destruction, loss or leakage of their data; Maintain a register listing all data processing operations; Analyze the impact of risky digital processing

				;
				Designate a delegate à the protection of data (*DPO*) for companies. Depending on the category of infringement, the fine ranges from 2% to 4% of the company's annual consolidated worldwide sales (or from 10 to 20 million euros).

In Community law, the RGPD provides, in its 176 introductory recitals and 99 articles, to make data fluid on a European scale. This is why the choice of a Regulation rather than a Directive was favored to promote such harmonization, which in practice proves not to be very intuitive for Internet users. The Regulation applies to all data controllers[653] , companies, public institutions and associations[654] , whether they are based in the EU or simply target European residents[655] . The various players in the digital environment now find themselves obliged to observe a multitude of fundamental principles and criteria defined by the RGPD, including a right to erasure, portability, data transparency, data retention periods, individual consent, a right to rectification, data controller liability and a right to information. Article 5 stipulates that "*Personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed* [data minimization principle]"[656] . This principle represents a security grail that has been identified as a cornerstone of personal data management and protection, particularly in view of the new IT concept of decentralized digital identity. In addition to the above considerations, there are at least three main situations that need to be taken into account in order to justify the collection, commercial use or disclosure of personal data.

[653] CNIL, European Data Protection Regulation, Chap. 4, Data controllers and processors, art. 24, accessed online on November 10, 2021.
[654] CNIL, "The data controller is the legal entity (company, municipality, etc.) or natural person who determines the purposes and means of a processing operation, i.e. the objective and the way in which it is carried out. In practice and in general, this is the legal entity embodied by its legal representative", consulted on October 19, 2022, at the following address
[655] JEAN Aurélie, "Do algorithms make the law?", "In this, the RGPD has overturned the rule that previously looked at the place of data storage only", reading position in the book: 86%.
[656] CNIL, Corrigendum to Regulation (EU) 2016/679, OJEU L127 2 of 23/05/2018, art. 5.1-c: principles relating to the processing of personal data, CHAPTER II - Principles, accessed online on September 15, 2021.

other forms of lawful processing of personal data in accordance with Article 6 of the Regulation[657] . Firstly, processing may be based on the performance of a contract to which the data subject is a party, or on pre-contractual measures taken at the data subject's request. Secondly, processing may be necessary for the purposes of the legitimate interests pursued by the controller or by a third party, unless the interests or fundamental rights and freedoms of the data subject prevail. Finally, processing may be required by law or necessary for the performance of a task in the public interest, or to safeguard the vital interests of the data subject or a third party. If the processing does not correspond to the above-mentioned points, then it can only be carried out with the consent of the person concerned. In this respect, cookies[658] and online advertising today target individuals without their consent being fully free and informed[659] . It should be noted that there is no article prohibiting the storage of biometric data on centralized servers, provided that sufficient safeguards and levels of security have been adopted to address the specific risks involved. Any negligence or breach will result in sanctions, followed by a formal notice from the CNIL[660] . If the resources deployed by the data controller(s) were insufficient, a fine of up to 2% of the group's consolidated worldwide sales or 10 million euros may be imposed[661] . In the event of a personal data breach, the fine may be as high as 4% of the group's consolidated worldwide sales, or 20 million euros of the group's consolidated worldwide sales[662] . Two years have passed between the adoption in 2016 of the RGPD and its application in 2018, a delay put in place to give European digital players time to comply. In reality, the CNIL has issued truly dissuasive sanctions from 2019[663] . Many websites have complied, but the strict application by design of the Regulation for some of them is still insufficient. Its legal effectiveness remains variable depending on the players involved. In 2021, Google was fined 100 million euros by the CNIL[664] with an increase in fines in recent years[665] , including the 125,000-euro fine levied against

[657] CNIL, RGPD, Chapter II - Principles, art. 6, accessed online on November 10, 2021.
[658] For more information on cookies and other tracers, *see* the CNIL website at the following address
[659] Note that prior to the application of the RGPD online consent was mostly tacit, i.e. the mere fact of browsing a website for a certain amount of time assumed the person's tacit consent.
[660] According to Article 83 of the RGPD, a formal notice can thus be damaging for targeted entities in terms of brand image and because of the public nature of the sanctions imposed by the CNIL, *v.* the list of sanctions on the CNIL website, consulted online on November 10, 2021.
[661] "Penalties and fines for non-compliance with the RGPD", in *LegalPlace,* online, published March 23, 2018, accessed November 10, 2021.
[662] CNIL, "Sanctions", consulted online on November 10, 2021.
[663] *Ibid.* Available at the following address
[664] CNIL, "Cookies: le Conseil d'État valide la sanction de 2020 prononcée par la CNIL contre Google LLC et Google Ireland Limited", Accessed on October 20, 2022, at the following address
[665] VITARD Alice, "With 1.2 billion euros in fines, will 2021 mark a turning point in RGPD compliance?
?" in *usine-digitale.fr*, "In 2021, the amount of fines imposed within the EU under the RGPD was multiplied by 7 compared to the previous year. It reached 1.2 billion euros with the record sanction of 746 million euros imposed on Amazon by Luxembourg", January 28, 2022.

of the Cityscoot company[666] for failing to comply with its obligation to ensure data minimization in violation of Article 5.1.c of the RGPD, following on from that of €175,000 pronounced against the short-term car rental company UBEEQO[667] . In reality, the CNIL's means of control remain derisory for breaches of European citizens' personal data (only 145 sanctions handed down by the CNIL since 2011, an average of around 13 sanctions per year)[668] . Also, some foreign companies manage to circumvent the application of the RGPD, a practice with which the CNIL was confronted in spite of itself at the beginning of 2023[669] .

Admittedly, while application of the GDPR is slow, it is progressive and structural for players operating in the digital sphere. Indeed, the Regulation serves as a benchmark for other data protection regulations, such as in China and California (see below). In this respect, the RGPD is contributing to a form of digital weaning for web players over the massive harvesting of personal data from Internet users. In 2019, the International Organization for Standardization (ISO) is launching a standardization initiative to establish guidelines for the protection of personal data in response to the adoption and implementation of the RGPD. This standardization movement aims to support the application of other personal data protection legislation inspired by the RGPD, such as the PIPL[670] adopted in China and the CCPA[671] adopted in the United States[672] . ISO/IEC 27701 standards[673] complete the certification process, enabling a privacy management system to be recognized as part of the management of risks linked to the processing of personal data. These standards are designed to be as broad in scope as possible. The RGPD only concerns natural persons and not legal entities[674] , which is a gap that decentralized identity could help to fill. In many use cases, the digital identity attributes of legal entities, such as their sales figures, accounting statistics and geolocation data, are collected and then resold

[666] CNIL, "Géolocalisation de scooters de location : sanction de 125 000 euros à l'encontre de CITYSCOOT", March 16, 2023, Citysccot collected scooter geolocation data every 30 seconds, available at [667] BOURDAIS Gaëtan, "Géolocalisation de véhicules : le gendarme CNIL contrôle!", in *Shift avocats*, March 29, 2023. Available at
[668] CNIL, "Les sanctions prononcées par la CNIL, année 2022", consulted on October 20, 2022, at the following address
[669] TAZROUT Zacharie, "La CNIL met en lumière une possible faille du RGPD", in *Siècle Digital*. January 25, 2023, available online
[670] The Personal Information Protection Law (PIPL) is a law adopted on August 20, 2021 in China. It is inspired by the European RGPD to provide a first law dedicated to the protection of Chinese citizens' personal data.
[671] California Consumer Privacy Act (CCPA) passed in 2018 and effective January 1er 2020 in several US states, in *US State Privacy Legislation Tracker*, accessed online January 19, 2022.
[672] Although each legislative text confers recognition and protection on personal data, their scope and application differ considerably, not least because of their respective titles. For example, the CCPA protects individuals as consumers, while the RGPD protects individuals and their data against any breach of their privacy. What's more, the penalties for violating the CCPA are low-deterrent and derisory, ranging from $2,500 to $7,500 per violation, compared to the stricter penalties applicable under the RGPD. The RGPD is more guided by a humanistic purpose, while the CCPA pursues a capitalist purpose, *see supra*, II, Title 1, 2.2.6
[673] Standard published in August 2019 extending the scope of the Information Security Management System
- ISO 27001 ISMS to ensure the protection of personal data. This standard is an extension of ISO/IEC 27001 and ISO/IEC 27002.
[674] Recital 14 of the GDPR states that "the protection conferred by this Regulation should apply to natural persons (...)".

without the transparency or consent of the representatives and managers of these legal entities. In other words, the collection and use (resale) of this data takes place without the necessary trust. It would be desirable for the RGPD to provide greater protection for certain data held by legal entities, or to clarify the notion of consent by a natural person acting on behalf of a legal entity. To address this issue, IN Groupe, Orange and Agdatahub are offering a novel decentralized digital identity solution called "Agriconsent"[675] . Thanks to decentralized digital identity, farmers can now manage their personal data autonomously and with complete confidence, both as individuals and as representatives of legal entities generating multiple sensitive data, as mentioned above. To this end, a specific mobile application can be used to issue and revoke verifiable attestations, explored further below, linked to a private blockchain to manage the professional activities of farms (applications for phytosanitary certificates, life cycle of a farm with the RCS, for example). The RGPD could thus be amended to reinforce the deployment of such solutions.

Originally, blockchain technologies were intended to free people from the principle of authority, as we have discussed. Conversely, the RGPD requires responsibilities to be identified and then clearly designated in terms of personal data management. Due to the absence of an intermediary and therefore of a data controller in a digital protocol such as a blockchain, the RGPD seems incompatible with this technology[676] . What's more, the cryptographic tools used by blockchains, which by design promote the pseudo-anonymity of Internet users, are not infallible and may make it possible to directly or indirectly re-identify a natural person[677] . As a reminder, any blockchain technology requires the native use of a public key, which in certain situations represents a means of identification for its users. This public key is systematically registered and recorded in a blockchain to enable unforgeable cryptographic sequences. Similar to a digital identifier such as an *IP* ("*Internet Protocol")* address, a public key may thus be subject to certain legal constraints with regard to the RGPD (see table below). According to European case law[678] and French case law[679] , an IP address represents personal data, which means by transposition that a key

[675] "Agdatahub: a digital identity on blockchain for the agricultural world". March 2, 2022, [Video]. Available on YouTube
[676] CNIL, "Premiers éléments d'analyse de la CNIL - Blockchain", September 2018, accessed online 04/10/2021, p.2, "Blockchain technology's decentralized data governance model and the multiplicity of players involved in data processing make it complex to define everyone's roles."
[677] It should be noted that online services and e-mail systems (Gmail, Outlook) are not, in principle, devoid of all personal data and include the first and last names of recipients, even though decentralized identity can make it possible to ensure correspondence with a recipient without possessing some of his or her personal information.
[678] CJEU, Judgment of the Court (Grand Chamber) of January 24, 2008, (Case C-275/06) in which the Court was asked to give a preliminary ruling in the dispute between the association Promusicae and the company Telefonica (Italian) concerning its refusal to disclose personal data relating to the use of the Internet to the means of connection provided by it.
See also ITEANU Olivier "Quand le digital défie l'Etat de droit", Ed. Eyrolles, where the author cites this CJEU ruling, pointing out that the CJEU consequently recognizes that an IP address is personal data.
[679] Cass. civ. November 3, 2016, 15-22.595, Published in the bulletin | La base Lextenso, accessed online on November 10, 2021.

public key could also be (in the same way as a VC and DID, discussed below). If a public key qualifies as personal data, then a blockchain must be considered as dealing with personal data. Similarly, according to the *Article 29* Data Protection Working Party (G29)[680] , certain adjacent cryptographic techniques such as hashing[681] may qualify as personal data and thus be subject to the GDPR depending on the situation, as the following table suggests. Even if an actor uses private and public keys to sign transactions and timestamping algorithms to guarantee data integrity on a blockchain, this does not mean that personal data is not processed. Pseudo-anonymity is not totally secure, and in certain circumstances it may be possible to identify an individual indirectly. Consequently, the application of the principles and requirements of the RGPD is unavoidable for blockchain technologies, a requirement that not all public blockchains meet to date. As such, we assume that some public blockchains will develop new updates whose legal compliance could be partial or total, as based on cryptographic commitment solutions and/or ecosystems of compliant and dedicated trusted third parties. Today, this quest for compliance by Web 3.0 players is, admittedly, in its infancy, but too widely underestimated by legal experts. As the following table shows, depending on whether the blockchain is public, private or hybrid, the rights of individuals mentioned under the RGPD do not apply in a systematic or linear way:

[680] *Op. cit,* "Article 29 Working Party | European Data Protection Board", in "L'identité numérique: quelle définition pour quelle protection?

[681] As a reminder, *hashing* is a condensed proof of encrypted data which, in principle, leads to anonymization of the original information (post-encryption). TechTarget, "Hachage (hashing)", in *LeMagIT*. Accessed June 12, 2022, at the following address, "Hashing is the transformation of a string of characters into a value or key of fixed length, generally shorter, representing the original string. Hashing is used in particular to index and retrieve items from a database. This is because it's quicker to find the element based on the reduced hash key rather than the original value. This function is also used in many encryption algorithms.

Type of blockchain (1/2)	Consent	Rectification	Collection of personal data	Clearly identified responsibilities	Technical authorizations and related rights
Public	Yes	No	No / Partially	No	Yes / Partially
Private	Yes	Yes	Yes / Partially	Yes	Yes
Hybrid	Yes	Yes / Partially	Yes / Partially	Yes	Yes

Type of blockchain (2/2)	Limited shelf life	Right to be forgotten/erased	Data portability[682]	Data accessibility and openness
Public	No	No	Yes / Partially	Yes
Private	Yes	Yes	Yes / Partially	No / Partially
Hybrid	Yes	Yes	Yes / Partially	No / Partially

A few remarks should be made about the right of rectification. In theory, it is computationally difficult to strictly modify or delete a block from a blockchain, as this would violate its principle of immutability and cryptographic chaining (of previously validated blocks). In practice, however, it is possible to add a new transaction to correct an existing entry, which can be done within the framework of smart contracts offering such functionality. As a reminder, this functionality within an AEC (smart contract, discussed in the previous chapter) must be provided for right from the initiation of the blockchain protocol in question. Similarly, in view of the

[682] ALIAS, "La portabilité des données: le droit oublié du RGPD, le rapport qui dénonce les ratés du RGPD contre les GAFAM", 2022, in *Global Security Mag Online*, available at.

principle of a right to forget/erase personal data, the minimization and encryption of such data contained in a blockchain seems unavoidable in 2022. To achieve practical, RGPD-compliant use, a principle of destruction (temporary use then destruction) or parcelling of the encryption key remains possible. These methods render personal data[683] indecipherable and unreadable respectively. In this respect, the CNIL recommends strict compliance with the principle of data minimization[684] , including through the use of cryptographic engagement. While these cryptographic pseudo-anonymization methods for personal data are difficult to implement, an impact study must nevertheless be carried out to identify whether the risks are acceptable. It is worth noting that the Estonian private and state blockchain has partially succeeded in resolving the problem of respecting the right to be forgotten, by introducing a specific rule that is binding on all parties involved in managing this infrastructure. In the event of a data proof being anchored on this chain, any modification to this transaction must enable its author to be identified. While this solution does not strictly meet the legal criteria of the right to be forgotten, including with regard to public blockchains, it does ensure a form of information obligation and then strict traceability for the managers of state-owned private blockchains. This principle of increased transparency could thus inspire certain public blockchains anxious to comply at least partially with this rule of law. To complement the table and the preceding sections, it seems important to complete and insist on the role and responsibility of three players essential to any blockchain infrastructure:

(i) Computers, nodes and validators[685] : these are the people who make physical and material computing resources available to run a blockchain protocol. While the existence of validator nodes is essential for any blockchain, their participation in the protocol does not necessarily mean that they qualify as processors. Indeed, this is open to interpretation, particularly in the case of public blockchains, where validators merely validate transactions automatically and indiscriminately via one or more software programs, whose underlying rules and responsibilities cannot be systematically imputed to them.

(ii) Developers: these Internet users and natural persons use their unique technical skills, generally assumed or pseudo-anonymously, sometimes anonymously, to participate in computer development.

[683] CNIL, "Premiers éléments d'analyse de la CNIL - Blockchain", *op. cit,* "lorsque un engagement cryptographique est parfaitement indistinguable (parfaitement hiding), la suppression du témoin et de la valeur engagée est suffisante pour anonymiser l'engagement de telle sorte qu'il perde sa qualification de donnée à caractère personnel", footnote 2.
[684] *Ibid:* "The principle of minimization states that personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.
[685] V. Appendix 6, Focus 1 to 3.

of a blockchain. Generally covered by multiple free licenses and open source codes, these communities of developers represent the essence of any blockchain. They therefore seek to attract as many developers as possible to their protocols and software ecosystems in order to ensure their technological and, by extension, commercial continuity (while at the same time reducing the social centralization of their developer community, as described above). However, the more developers there are, the more complex and political this algorithmic governance becomes. This often involves internal power struggles, an observation that the Bitcoin developer community has been experimenting with for 14 years[686] , the Ethereum community for 7 years, and the consortium and private blockchain communities more recently.

(iii) Users: these are mainly Internet users whose personal data (generally pseudo-anonymized[687]) is processed by the blockchain systems they use. Each Internet user is thus largely dependent on the two previous players to carry out transactions, which explains why legislators wish to protect consumers with a strict legal framework for their personal data.

Consequently, while blockchain technologies advocate the decentralization of trusted third parties, there is often a data controller who must respect certain legal principles specific to the collection, processing and retention of personal data, particularly in the case of closed, centralized blockchains, as confirmed by an EBSI report[688] . With regard to the liability associated with decentralized digital identity (IND) solutions, discussed below, in the event of a dispute, a judge may first investigate whether a specific liability regime applies

[686] Bitcoin has a proven and growing community, as bitcoin analyst and miner Guillaume Girard of Galaxy Digital explains on his personal blog: "Many people criticize maximalism as a form of extremism and closed-mindedness, but if the short history of CryptoTwitter teaches us anything, it's that for a community of individuals to be inspired to stand up and fight [...], it needs to be united by simple values. When Bitcoin's core values came under attack, we needed maximalists to stand up and lead the charge against an organized enemy. [...] However, Maximalism, in the form of Extreme Order, must remain an emergency measure. [...] I implore my fellow Bitcoiners and Ethereans to be maximalists of rabid decentralization", "A tale of chaos vs order: the ideological war between Bitcoin and Ethereum doesn't need to happen", 2022, accessed at the following address. While the community maximalism on which Bitcoin is based is necessary for its computational and economic stability, it is likely that this social movement will be diluted over time by the late majority of non-maximalist new entrants (general public, companies, institutions, states, etc.). For the Bitcoin blockchain, the complexity thus lies in the inevitable conduct of this coming community and social change, rather than in the protocol's quest for IT resilience, which has already been achieved.

[687] Anonymization techniques refer to ways of transforming datasets - deleting certain attributes, generalizing, noise suppression and other manipulations - in order to make it very difficult, if not impossible, to re-identify or infer knowledge about individuals.

[688] EC, "EBSI GDPR Assessment, Report on Data Protection within the EBSI Version 1.0 Infrastructure", pp7- 8, translated freely from English, "[data controllers] must take all necessary measures to ensure that data subjects are sufficiently informed and have the opportunity to exercise their data protection rights", consulted on 23/03/2022 and available at the following address, *v. supra,* I, Title 1, 2.2.2.2

to the given situation. If no specific regime applies, he will then determine whether the conditions for contractual liability are met, which will often be the case for the supply or use of decentralized identity solutions. However, if the latter is excluded, tort liability may nevertheless be sought, depending on the specific case. Public blockchains are accessible to all users, which means that every validator participating in the consensus could be considered a data controller in the event of a data breach, money laundering or terrorist financing. However, the legal reasoning currently used to identify data controllers is insufficient when applied to the validators of a public blockchain. Therefore, a detailed legal impact analysis needs to be carried out for each blockchain to identify the true data controllers in terms of governance[689] , rather than direct IT processing.

Despite a few observations and the perplexity of the doctrine, partly due to a difficulty in the legal interpretation of blockchain technologies, the CNIL has issued an unavoidable opinion on the use of blockchain technology for the purposes of the RGPD. It considers that all blockchain technologies are compatible with the Regulation. In terms of identifying data controllers, it states that actors who possess "(...) *a right to write on the chain and who decide to submit data for validation by miners can be considered as data controllers*"[690] , specifying that an actor [validator or developer] is a data controller stakeholder as soon as it "*determines the purposes (the objectives pursued by the processing) and the means implemented (data format, use of Blockchain technology, etc.)*". Still according to the CNIL, "*a permission Blockchain* [hybrid blockchain] *should be preferred, as it gives greater control over the governance of personal data, particularly with regard to transfers outside the EU*", as "*binding corporate rules or standard contractual clauses are fully applicable in a permission Blockchain*". Indeed, in June 2021, the European Data Protection Committee (EDPS) published a series of "additional protections" that led the Commission to repeal the old contractual clauses (CCTs) and adopt new ones. The CNIL also states in concluding remarks that "*particular vigilance should be paid to the measures implemented to ensure the confidentiality of the Blockchain if it is not public*"[691] . In this respect, while the majority of private and hybrid blockchains are therefore not decentralized, they are by design RGPD-compliant and, as such, favored by players seeking legal compliance. According to the aforementioned G29 working group on data protection, the status of data controller within a technology

[689] V. Appendix 3 and Appendix 6, Focus 1 to 3.
[690] CNIL, "Premiers éléments d'analyse de la CNIL - Blockchain", *op.cit.* p.7. accessed online.
[691] *Ibid*. p.7.

blockchain can be acquired or assigned as soon as each node acts as a processor or controller of data, i.e. by participating directly or by delegation in its processing. In addition, the report dedicated to the RGPD of a European blockchain (EBSI) states "in the *event of joint control, data controllers may contractually assign partial responsibility on the basis of distinct stages of data processing*"[692] . If an agreement between these data controllers exists and allows each responsibility to be defined, then "*data subjects shall be able to exercise their rights against each joint controller*" and "*the nodes that add and process data to the on-chain ledger* [master blockchain protocol] *in order to maintain the consensus shall be individually qualified as joint data controllers and this, regardless of a contractual relationship stipulating otherwise*".

Focusing on decentralized digital identity, and more specifically on the use of decentralized digital identifiers (DIDs), which are studied below, representing digital identifiers in the sense of the CNIL, the latter "*considers that it is not possible to minimize them* [the identifiers] any *further and that their retention periods are, in essence, aligned with those of the Blockchain's lifespan*"[693] . Today, this consideration is partially outdated, i.e. it is possible to use "*cryptographic commitment mechanisms*" that guarantee a high degree of protection against any attempt to re-identify their beneficiaries. As a result, decentralized identities (DIDs) not only represent cryptographic commitment mechanisms within the meaning of the CNIL, but also appear to be in line with the principle of minimizing digital identifiers based on a blockchain. Internationally, there is debate as to whether decentralized identifiers, which are not yet uniformly considered personal data in different jurisdictions, can be stored as is or as a "hash"[694] on a blockchain. The question of whether a hash constitutes personal data remains controversial, and national data protection agencies are struggling to define clearly whether hashing can be considered a sufficient anonymization mechanism, or rather a pseudo-anonymization mechanism. This debate is likely to continue over the next few years. The smart contracts (AEC) discussed in the previous chapter are also relevant to the development of a decentralized identity solution, particularly with regard to the management of decentralized digital identities and verifiable credentials, the latter of which are discussed in detail in the next section of this study. In principle, the appropriate measures[695] mentioned by the CNIL to guarantee the availability of such 3.0 solutions in real-life IT environments are

[692] "EBSI GDPR Assessment, Report on Data Protection within the EBSI Version 1.0 Infrastructure", *op. cit.*
[693] *Ibid*. p.7.
[694] See *above,* Title I, 2.3.1.1.b
[695] Art. 32 RGPD: "[...] the controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including as necessary: [...] means to restore the availability of and access to personal data within appropriate timeframes in the event of a physical or technical incident".

hybrids (multiple technological layers), imply a certain difficulty in implementation. For example, a user should be able to obtain human intervention, express his or her point of view, or contest a validated transaction after the execution of an intelligent contract (AEC mentioned above). In other words, negotiation must be possible. The data controller should therefore be able to provide for the possibility of human intervention to challenge the transaction carried out, by granting the data subject the right to challenge the transaction "*even if the contract has already been executed, and this independently of what is recorded in the blockchain*"[696] . In reality, while this is computationally feasible for private and hybrid blockchains, such functionality is complicated to implement for public blockchains due to legal compliance, which is not yet a core concern for these 3.0 developer communities. Complementing the above, the revised eIDAS Regulation (eIDAS-2) studied in the second part of this study, will impose greater protection for personal data. First of all, this revision imposes a principle of prohibition on the collection of 3.0 data resulting from the use of digital identity wallets (PIND), which are also studied in the second part of this study. Thus, the supplier of a PIND may not collect this 3.0 data, unless it is strictly necessary for its operation (updates). Similarly, limited combination of personal data is possible by these PINDs, i.e. their public (state) and private (corporate) providers will not be able to combine identification data with personal data from other services, unless requested by the user. Where a provider of a verifiable attestation is also a provider of an online service, the services provided will have to be with separate legal entities to prevent any possibility of correlation (re-identification) of personal data by the said online services. In addition, organizational measures must be in place to guarantee a high level of security and rapid notification to data protection authorities in the event of a data breach. Finally, the implementation of a certification or *trust mark* for the aforementioned PINDs is possible for each Member State, under the visa of Article 42 of the RGPD[697] . It should be noted that these legal recitals, which are based on the protection of individuals' personal data, are particularly binding for identity and online 3.0 service providers. In practice, these measures reflect a willingness to change the paradigm with regard to the processing of people's personal data, which allows for a form of optimism with regard to this third-generation digital identity.

When it comes to responsibility for managing a PIND, the report on data protection within the EBSI infrastructure[698] notes that "*there is a growing consensus that it is possible to*

[696] "Premiers éléments d'analyse de la CNIL - Blockchain", *op. cit,* p.10., consulted online
[697] Art. 42 RGPD, July 2, 2021, available at.
[698] "EBSI GDPR Assessment, Report on Data Protection within the EBSI Version 1.0 Infrastructure", *op. cit.* Accessed online November 10, 2021.

the individuals concerned to be simultaneously considered as data controllers". Consequently, a decentralized digital identity solution that tends towards a form of individual sovereignty would enable digital identity providers to exonerate themselves from all or part of their responsibility in the event of user fault in the administration of their data. The same report recommends that "*technical and organizational measures to preserve wallet privacy and personal data transmissions should ensure that the necessary safeguards are in place so as not to limit the empowerment of the person concerned by the chosen DLT* [blockchain] *model*"[699] . It should be noted that Article 109 of the French Data Protection Act of 1978, as amended, allows any person to exercise a right of access, rectification or opposition to his or her data by electronic means, once the data controller has collected it by this means[700] . Thus, verifiable attestations make it possible to comply strictly with these rules, thanks in particular to their revocable and sometimes temporary nature. Legal entities are covered by the eIDAS-2 Regulation and not, as already explained above, by the RGPD. Indeed, between the extensive protection afforded to natural persons and the non-existent protection afforded to legal persons by the RGPD, the introduction of protection for legal persons within eIDAS-2 represents a security in this sense. In other words, it avoids a form of disproportionate concentration of the digital identity attributes of legal entities (sales, activity data) by certain identity providers, as is already the case in certain industrial 2.0 sectors (banking, agriculture[701] , pharmaceuticals). Finally, the data contained in a decentralized digital identity wallet application will be considered personal data and therefore subject to the GDPR. Although there is a presumption of reliability that decentralized identity solutions would be RGPD-compliant by design, only court rulings and case law will confirm such an assumption on the basis of a case-by-case assessment. In the meantime, it is advisable to avoid the exposure of personal data on a public blockchain, by individuals not writing down their digital identifiers, as already suggested by certain self-sovereign digital identity solutions, studied in the second part of our study. In principle, blockchain technologies and the RGPD are not incompatible, as some legal experts assert[702] . In practice, the use of blockchain technology makes it possible to implement a form of

[699] *Ibid*. p.12.
[700] The information referred to in articles 104 to 106 shall be provided by the controller to the data subject by any appropriate means, including electronic means and, in general, in the same form as the request, available at the following address
[701] VITARD Alice, "Agdatahub, la plate-forme pour protéger et valoriser les données agricoles françaises", 2020, in www.usine-digitale.fr, *v.* the industrial use case for a decentralized identity offered by IN Groupe and Orange to French farmers.
[702] DEROULEZ Jérôme, avocat, "Comprendre les blockchains : fonctionnement et enjeux de ces nouvelles technologies", avocat, ″despite a mode of operation that is sometimes antinomic with the principles of data protection law, blockchain will perhaps paradoxically provide the technical solutions most capable of protecting this data in the digital age and guaranteeing the effectiveness of a law that is sometimes undermined in an increasingly complex and transnational technological environment", in *Sénat.fr*, consulted online 05/10/2021.

optimized data governance[703] , in line with the principles of the RGPD, provided that prior attention to its rules is given to projects involving blockchain technology and decentralized digital identity solutions. The consent of individuals strengthens their rights[704] , for example by allowing them to revoke[705] their digital attributes at any time and on their own initiative. The complementary nature of these 3.0 tools and technologies makes it possible to ensure the transparency of all or part of the digital identity value chain, provided that the main principles of these technologies and the RGPD are articulated and respected right from the design stage. Ultimately, while the postulate of compliance by design of closed blockchains is favored in this study, it is important to note that certain private or hybrid blockchains do not always comply with the texts in force, particularly financial law, for example when a "tokenization" of these infrastructures is envisaged. This can happen when the parties involved in the blockchain collectively decide not to prioritize compliance with the law for various reasons, although it should be remembered that this situation currently only concerns a minority of private and hybrid blockchains.

2.5 Community law at the service of policy: MiCA and TFR regulations

Since 2019, the European legislature has been taking an active stance and aims to position itself as a forerunner in the regulation and legal oversight of crypto-assets. Adoption of these digital assets varies considerably around the world (see Appendix 14), but according to a study conducted in 2022 by the European Central Bank[706] , around 10% of Europeans hold crypto-assets. These figures are in line with estimates of 6% to 8% of French people holding cryptocurrencies[707] . Switzerland, considered a pioneer in this field with its public institutions[708] , was quick to adopt an innovative and proactive legal stance. This is partly due to their flexible approach to regulating these 3.0 technologies, a strategy that is now bearing fruit[709] . By 2030, crypto-assets will probably be regulated in

[703] *Op. cit,* "Premiers éléments d'analyse de la CNIL - Blockchain", 2018, "In addition to minimizing the risks for the individual, seen above, the format [VC/DID?] chosen to write the data on a Blockchain may make it easier for individuals to exercise their rights", p.9, available at.
[704] See *infra*, II, Title 1, 2.2
[705] The notion of revocation is essential: in the event of misuse of one or more *verifiable certificates* (*VCs)*, revoking them and then renewing them (with a new certificate) limits any attempt at identity theft, while ensuring continuity (and the associated trust) for the person's digital identity.
[706] Speech to the ECB, April 25, 2022, "For a few cryptos more: the Wild West of crypto finance",
"This crypto-asset offering has generated strong demand from both professional investors and the public. By 2021, around 16% of Americans and 10% of Europeans," available at.
[707] Les Echos, May 24, 2022, "Un foyer sur dix en zone euro détient des crypto-actifs," accessed October 20, 2022, at.
[708] Swiss law is a benchmark for the adoption of crypto-assets, both in terms of regulations (clear legal qualification and support for crypto-asset service providers), and tax incentives (to attract investors and encourage innovation).
[709] GREGORY Raymond, "How Switzerland became the first crypto-nation", 2022, in *Capital*, accessed October 21, 2022, at.

all developed countries, whose legal frameworks generally trickle down and influence developing countries in a second phase. On October 5 and 10, 2022, the Council and European Parliament voted on two regulations, the MiCA Regulation[710] and the TFR Regulation[711] , which are due to take effect in 2024. Two specific sections are devoted to analyzing these texts in their political context, their analysis aiming to better understand the direct consequences of these rules on 3.0 technologies, applications and ecosystems. Since 2020, the European legislator has considered it essential to adopt new rules to provide a healthy and secure development environment for both citizens and professional players in the crypto-asset sector. However, the application of these rules requires appropriate means of supervision to ensure compliance, which has only been partially the case on a national scale since 2019[712] . Indeed, French digital asset service providers are obliged to comply with a registration and sometimes approval regime, known as PSAN regime(s), aimed primarily at warding off the risks of scams, money laundering and terrorist financing. This legal framework, orchestrated by the Autorité des Marchés Financiers (AMF) and the Autorité de Contrôle Prudentiel et de Résolution (ACPR), implies an overall cost of compliance that is substantial and often out of reach, for players with often modest resources and size. At the same time, some of the foreign players and crypto-asset service providers that dominate the market only began complying with its new rules from 2021, while continuing their activities aimed at the national and European market, without having been PSAN-registered with the AMF at that time. In other words, this handful of foreign players were allowed to pursue unregistered activities well after other French players faced with compliance obligations. The current legal regime, recently reinforced by the DDADUE law[713] , has allowed free competition between PSAN players registered in France, and those foreign players not registered but still operating illegally in France for several years in some cases. Today, it seems that the PSAN regime has not particularly mitigated the side-effects of recent international crypto-asset scandals (scams, mismanagement, chain liquidity defaults). After almost five years of hindsight (2019-2023), the national legislator seems partly responsible for this situation according to national players in this ecosystem represented by the Association for the Development of Digital Assets (ADAN), proactive on the subject. In fact, it seems that the legislator created this regime of rules

[710] Proposal for a Regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937, available at the following address, *see* also the section on the MiCA Regulation below.
[711] Proposal to recast Regulation (EU) 2015/847 "Transfer of Funds Regulation", available at the following address, *see* also the section on the TFR Regulation below.
[712] *Op. cit.* GASSER A, MOULIN J-M, QUINIOU M., et al, "La Finance Numérique - Aspects juridiques et fiscaux du crowdfunding et des cryptoactifs", p. 146, "L'AMF manque de moyens pour faire appliquer le dispositif des *Prestataires de Services sur Actifs Numériques (PSAN)* instauré par la *loi Pacte* en 2019. The minimum time required to process a PSAN registration application is six months, a period during which the future PSAN cannot operate in accordance with this legal regime."
[713] Loi n°2023-171 du 9 mars 2023 portant diverses dispositions d'adaptation au droit de l'Union européenne dans les domaines de l'économie, de la santé, du travail, des transports et de l'agriculture. JORF March 10, 2023, v. Cabinet avocats Gide Loyrette Nouel, "Loi DDADUE : renforcement du régime applicable aux futurs PSAN enregistrés", 2023, available at

without providing the relevant authorities (AMF and ACPR) with sufficient means of control and verification when the PACTE law came into force, which introduces mandatory registration in addition to optional approval for certain activities relating to crypto-assets (listed in the CMF). Without adequate means to enforce these rules, new regulations may be a source of loss of competitiveness for certain players in this ecosystem[714] . The following paragraphs attempt to explain the extent to which the rules currently being adopted or recently adopted by the EU remain necessary in the face of infringements of Internet users' personal freedoms. It explores how the concept of technological neutrality is enshrined in these texts relating to crypto-assets and their ecosystems of providers, i.e. mainly concerning public blockchains with a financial vocation. We find that, while regulating the players in these ecosystems is essential given the current state of the technologies and their uses, attempting to prohibit them (through rules of law and/or political principle) represents a technological and social contradiction, and would also result in economic counter-productivity. National regulation of crypto-assets, itself partly inspired by Swiss law[715] , was a source of inspiration for the European legislator in creating the MiCA Regulation and the proposed amendment to the TFR Regulation, although certain financial[716] and energy considerations (*see* Appendix 6) seem to be leading to a political desire to limit the adoption of crypto-assets. The following two sections examine whether the MiCA and TFR Regulations are really institutional attempts to prohibit in law and/or in practice certain IT protocols or providers of these 3.0 ecosystems, deemed too complex to regulate due to their high degree of decentralization (*see* Appendix 7). In its first versions, the MiCA Regulation had the political objective of considerably limiting the exploitation and use of the most decentralized crypto-assets (issuance, purchase and sale, holding and transfer), sometimes going so far as to propose banning them. In the end, European legislators opted for more precise, incentive-based rules that are legally perceived as proportional, while allowing the common market more than a year to adapt between the adoption and implementation of these texts. This long period of time will enable the preparation of a second "MiCA-2" text and other texts relating to DeFi, NFTs and crypto-asset mining[717] . The adoption of this constellation of regulations and texts will undoubtedly have a significant impact on the development of the blockchain technology market, and particularly on its financial and legal applications. However, it would appear that the aim is not to encourage

[714] Except for the biggest players, which are mainly foreign entities with the resources to comply with the rules as late as possible - often through lengthy political negotiations to avoid sanctions - the rules already in force are either applied minimally, or circumvented to avoid sanctions.
[715] LANGLOIS-BERTHELOT Thibault, BOUILLET-CORDONNIER Ghislaine, "Tour d'horizon du droit financier Suisse : Crowdfunding - ICO - STO", in *Albatross Legal*, pp16, available online.
[716] FLEURET Faustine, May 2, 2022, "Regulation kaMICAze in Europe?", "For years, there has been a strong belief [persists among European legislators] that digital assets represent a preferred vehicle for money laundering and terrorist financing, even though recent studies show the opposite," in *Grand Angle Crypto,* YouTube, 2022, available at.
[717] V. Appendix 6, Focus 1.

amalgams with political discourse based on the fight against money laundering and the financing of terrorism, and the energy-hungry nature of certain blockchains[718] , so as not to hinder certain freedoms such as innovation and entrepreneurship, at the risk of engendering a loss of fundamental rights or even a massive flight of talent and capital abroad.

2.5.1 Proposed Markets in Crypto-Assets Regulation (MiCA)

Stemming from a series of measures relating to the legislative package on digital finance in Europe or "*Digital finance package*"[719] , the European Regulation on crypto-asset markets or "*Markets in Crypto-Assets - MiCA*" was presented on September 24, 2020 by the European Commission[720] . It is part of a broader, European drive for political support regarding blockchain technology[721] . Its nine titles aim to frame crypto-assets by creating a European regulatory framework that promotes technological development while ensuring financial stability and consumer protection within the EU. While some EU member states already have a national framework governing crypto-assets, MiCA is intended to replace them, including the French regime governing public offerings of tokens ("ICOs") and digital asset service providers PSAN[722] aforementioned. While some of these rules will apply without difficulty under domestic law, others will need to be adapted in line with the new strict rules. The aim of the MiCA Regulation is to provide an EU-wide framework for crypto-asset service providers[723] , including for specific, unregulated segments of this market (certain non-fungible tokens and stable crypto-assets[724]). This involves registering all players in this ecosystem, regardless of the EU country from which they operate. This involves categorizing each type of asset and associated player, within a harmonized legal framework in terms of consumer protection and European competition[725] . The aim of this Regulation can be summed up in several objectives:

---

[718] FLEURET Faustine, *op. cit*, " Il y a encore beaucoup d'institutions qui pensent que la crypto est un véhicule préféré pour le blanchiment et le terrorisme; pour l'écologie c'est le même constat ", in *Grand Angle Crypto,* YouTube, 2022 at the following address

[719] European Council. "Digital finance package: Council reaches agreement on MiCA and DORA", 2021, available at

[720] *Op. cit,* "Proposal for a regulation of the european parliament and of the council on Markets in Crypto-assets amending Directive (EU) 2019/1937 COM/2020/593". MiCA is part of the "Digital Finance Package", which aims to transform the European economy over the coming decades. Available at

[721] *Ibid*. This initiative is closely linked to broader Commission policies on blockchain technology, as crypto-assets, as the main application of this technology, are inextricably linked to the promotion of blockchain technology across Europe. This proposal supports a comprehensive approach to blockchain and DLT, which aims to put Europe at the forefront of blockchain adoption and innovation."

[722] BOUILLET-CORDONNIER Ghislaine et al, "La Finance Numérique, aspects juridiques et fiscaux du crowdfunding et des cryptoactifs", *op. cit,* p.146.

[723] *Op. cit.* MiCA, art. 3.1 (8): "crypto-asset service provider: any person whose occupation or activity consists in providing one or more crypto-asset services to third parties on a professional basis".

[724] See *supra*, II, Title 2, 2.4.

[725] Implementing a minimum equity threshold for these platforms, technical requirements and transparency and control of their governance. These rules imply costly resources and progressively recentralize public blockchain ecosystems, which is both desirable from a legal point of view, and harmful from an IT point of view.

harmonize national legislation in favor of a Community approach to these assets[726] , ensure legal certainty, protect consumers, prevent fraud and guarantee financial stability within the EU. In practice, the MiCA Regulation provides for mandatory approval of *Crypto-Asset* Service Providers (CASP*)*. Its requirements are similar to those of the optional French PSAN regime mentioned above. Thanks to this new Regulation, which is thus inspired by the Swiss and French legal regimes, approved CASPs will benefit from a "*European passport*"[727] enabling them to provide and operate their services in all EU countries, rather than having to comply with each national legislation (which is currently complex and costly for crypto-asset platforms/exchanges). As such, in France they will need an authorization issued by the competent national authorities (the AMF) within three months, in order to operate freely within the EU thanks to this normative passport. To ensure the traceability and transparency of these 3.0 players, a public register[728] of PSCAs registered with the European Securities and Markets Authority (ESMA)[729] will be available on the Internet. MiCA introduces further measures, such as the requirement for customers' crypto-assets to be segregated from funds belonging to the PSCA and protected in the event of insolvency. At the same time, these players will be subject to regular transmission of information between the competent authorities, notably the European Banking Authority (EBA), which will be responsible for maintaining a public register of PSCAs that do not comply with the FATF's proposals on money laundering and terrorist financing risks[730] . In this respect, we would point out that these exchanges of sensitive, inter-organizational information between multiple national, community or international bodies can make use of decentralized digital identity (IND) solutions, discussed below, to guarantee the confidentiality and integrity of the data exchanged. Similarly, token issuers[731] can use these digital identity 3.0 mechanisms as part of their obligation to have a "*robust internal control and risk assessment mechanism",*

[726] *Op. cit.* MiCA, (Background to the proposal): "while [prior to the adoption of MiCA] certain crypto-assets may fall within the scope of EU legislation, it is not always straightforward to apply this legislation to them in practice", available at

[727] Gide Loyrette Nouel, avocats, "Agreement reached on European crypto-assets regulation (MiCA) under the aegis of the french presidency of the European Union", in *gide.com*, July 1, 2021, available at.

[728] *Op. cit.* Proposed Regulation 2019/1937 (MiCA). Art. 57: "ESMA shall maintain a register of all crypto-asset service providers. This register shall be publicly accessible on ESMA's website and regularly updated, *see* also recital (53) : In order to promote transparency for holders of crypto-assets with regard to the provision of crypto-asset services, ESMA should set up a register of crypto-asset service providers, which should contain information on entities authorized to provide these services throughout the Union. This register should also include white papers notified to the competent authorities and published by crypto-asset issuers", available at the following address

[729] The European Securities and Markets Authority, created in 2011, is an independent EU authority that aims to improve investor protection and promote the stability and smooth operation of financial markets, see european-union.europa.eu (ESMA).

[730] In this respect, it is emphasized that PSCAs whose parent companies are located in countries on the EU list of third countries considered to be high-risk in terms of anti-money laundering activities, or on the list of fiscally non-cooperative jurisdictions, will be required to implement enhanced safeguards and controls.

[731] *Op. cit,* MiCA, art. 3, 1. (6) "issuer of crypto-assets: a legal entity that offers any type of crypto-assets to the public or applies for admission of such crypto-assets to a crypto-asset trading platform".

[732] . In this respect, we suggest that decentralized identity should become the cryptographic rule to meet these new institutional and commercial constraints imposed by the MiCA Regulation. Indeed, applying a digital identity 2.0 to these exchanges of highly sensitive information on an industrial scale may pose problems of an IT nature (known risk of massive data leakage), and also of a geopolitical nature (digital sovereignty not respected if these data exchanges are carried out via federated digital identities that depend on GAFAM/BHATX as we have mentioned). In terms of sanctions, article 92 of MiCA stipulates that the competent authorities of each country may, in accordance with their supervisory powers, penalize any infringements. Heavy fines of between 500,000 and 700,000 euros are provided for in the event of non-compliance. For legal entities, penalties may be set at between 5 and 15 million euros and/or 5 to 15% of the total consolidated annual sales of the legal entity concerned.

March 14, 2022 is a symbolic date for the European crypto-asset ecosystem, and by extension for all adjacent Web 3.0 ecosystems. Indeed, this date marks the day when MEPs rejected in extremis some alarming proposed amendments to the initial version of the proposed MiCA Regulation[733] . These proposals to insert earlier articles into the draft regulation were put forward by certain members and MEPs of the European Parliament's Committee on Economic and Monetary Affairs. One of them, not very pragmatic, suggested that only crypto-assets complying with "*minimum environmental sustainability standards*" could be issued, offered or admitted to trading within the European Union[734] . With this provision, it would have been required that certain crypto-asset infrastructures already issued and accessible to the public, such as bitcoin[735] since 2009 and ether[736] since 2015, put in place and maintain a progressive roll-out plan[737] to ensure compliance with certain minimum environmental requirements. If this had been possible for the Ethereum blockchain and its actually semi-decentralized ecosystem (in reference to its foundation)[738] , the degree of pure decentralization of Bitcoin and its *Proof of Work ("PoW*") mechanism[739] , studied in Appendix

[732] *Ibid*. Recital (34).
[733] European Parliament News, "Econ Voting Sessions 14 March 2022", 24 votes for and 32 against, available at
[734] Art *2a* and *(5aa)* of the rejected version, available online at
[735] Mempool - Bitcoin Explorer, accessed October 24, 2022. View the first block of the bitcoin blockchain at
[736] The Ethereum blockchain was launched with the creation and validation of its first block: "Blocks #0", available on Etherscan at the following address
[737] In concrete terms, this involved publishing PDFs (White Papers) explaining how the aforementioned blockchain intends to reduce its CO2 emissions (documentation that Bitcoin cannot produce in its current state of operation and community).
[738] V. Appendix 7 & Appendix 6, Focus 2.
[739] V. Appendix 5.

6 (Focus 1), would not have been able to satisfy such legal requirements. Ultimately rejected[740] , the adoption of this proposal would have de facto led to a partial or even total ban on the mining, acquisition and storage of bitcoins or ethers. The motivation behind this proposal was that the Proof-of-Work mechanism would unnecessarily consume too much energy, a partially inaccurate assumption as demonstrated in this study[741] . Further political attempts to restrict the bitcoin mining industry are likely to emerge on the grounds of the industry's perceived disproportionate energy consumption, despite the fact that only 0.04% of the electricity consumed in Europe in 2022 will actually come from bitcoin mining[742] . A ban on this historic computing mechanism, specific to the first blockchain to date, would probably put an end to a significant part of the European blockchain ecosystem, which would therefore probably move to countries with more favorable jurisdictions. Still from Appendix 6 of this study, it seems that for several years now, the mining manufacturing industry, specific to some of the public blockchains studied in the Appendices, has been mobilizing to improve their respective energy footprints. In a few years' time, every mechanism and computer operation of open and/or closed blockchains will now be analyzed in a "*European green taxonomy*"[743] , thus encouraging the players concerned to improve their energy footprint through the use of renewable energies, without banning them, as several scientists proposed in a joint tribune in June 2022[744] . In this respect, it should be emphasized that this attempted ban concerns not only Bitcoin's energy consumption, but also its social utility, as the two are in fact inseparable, as Satoshi Nakamoto mentioned as early as 2010 in response to similar criticism on a blog[745] . Ultimately, the current version of the MiCA Regulation is the result of compromises between the European Commission and the European Parliament, which intended to include crypto-assets in the European taxonomy for sustainable finance. While common sense has finally won over a majority of MEPs by eliminating the initially envisaged ban on the Proof of Work mechanism, this is not enough to dispel concerns about PSCAs and their new environmental disclosure obligation.

[740] Following the vote on Monday, March 14, 2021 by the Economic and Monetary Affairs Committee (ECON) on the European Parliament's final compromise text, the text will not be contested in plenary.
[741] *Ibid*.
[742] STACHTCHENKO Alexandre, "That's 0.04% of European [...] electricity production [that Bitcoin would consume]. "2022, available on Twitter, see also Appendix 6, Focus 1.
[743] FLEURET Faustine, "Regulation and innovation in the field of cryptoactives - Round table", available on videos.senat.fr
[744] Institut Rousseau et al, tribune de chercheurs qui estiment qu'" Il est urgent d'agir face au développement du marché des cryptoactifs et de séparer le bon grain de l'ivraie [...] ne pas autoriser les cryptoactifs dont l'impact sur l'environnement est inutilement nocif", accessed June 1, 2022, at.
[745] NAKAMOTO Satoshi, "Bitcoin mining is thermodynamically perverse", August 7, 2010 "It's the same situation as with gold and gold mining. The marginal cost of gold extraction tends to stay close to the gold price. Gold mining is wasteful, but the waste is far less than the utility of having gold as a medium of exchange. I think the case will be the same for bitcoin. The utility of the exchanges made possible by bitcoin will far outweigh the cost of the electricity used. Therefore, not having bitcoin would be a net waste", available online at

These concerns persist until the publication of the draft regulatory technical standards[746] to be drawn up by the EBA and ESMA in the near future. In addition, it is noted that the environmental disclosure obligation imposed on PSCAs does not apply to traditional financial players and institutions, an obligation incumbent only on PSCAs[747] . In addition to the aforementioned new rules, the MiCA Regulation introduces ad hoc regimes for (i) non-fungible tokens (NFT/JNF), and (ii) stable crypto-assets ("*stablecoin"*)[748] .

(i) In principle, digital tokens that are unique and non-interchangeable, i.e. non-fungible (JNFs), are exempt from the scope of MiCA according to its annexes (notably for so-called artistic or collectible NFTs, which are excluded). In practice, national supervisors (AMF, ACPR) could requalify certain types of JNF on a case-by-case basis if their characteristics or uses are similar to the qualification of financial instruments or crypto-assets within the meaning of the present Regulation. In other words, the non-fungibility of an NFT may be questioned and requalified when it is issued in large quantities to the public, or when it can be split.

(ii) Faced with the progressive use of crypto-assets whose value is stable, or "*electronic money tokens*" as defined by MiCA[749] , more commonly referred to as "*stablecoins*"[750] , MiCA distinguishes between (a) "*tokens referring to assets*", (b) "*electronic money tokens*"[751] . Firstly, it regulates

[746] European Parliament, "News Cryptocurrencies in the EU: deal struck between Parliament and Council", June 30, 2022. Available at (5a), p.8, "the consensus mechanisms used to validate crypto-asset transactions could have major negative impacts on climate and other environmental impacts. These consensus mechanisms should therefore deploy more environmentally friendly solutions and ensure that any main negative impacts they may have on climate and any other negative impacts related to the environment are identified and adequately disclosed by crypto-asset issuers and service providers. In determining whether the negative effects are principal, the principle of proportionality and the size and volume of the crypto-assets issued should be taken into account. ESMA, in cooperation with EBA, should therefore be tasked with developing draft regulatory technical standards to further specify the content, methodologies and presentation of sustainability indicator information with regard to climate- and environment-related negative effects, and to define key energy indicators."

[747] *Op. cit,* "CASPs must make information about their environmental and climate impact available to the public in a prominent place on their website". While these requirements could in theory be met by the Ethereum blockchain and its Foundation, the Bitcoin blockchain could not, as no 'Bitcoin Foundation' or trusted third party administers it in any meaningful way.

[748] See *infra*, II, Title 2, 2.4.

[749] *Op. cit,* MiCA, Art. 3, 1. (4), "'electronic money token': a type of crypto-asset whose main purpose is to be used as a medium of exchange and which aims to retain a stable value by referring to the value of a fiat currency that is legal tender".

[750] CARRIER Anna, "Member States continue MiCA review", 2020, in *Regulation Tomorrow*, available at, art. 3, "crypto-assets primarily intended as a means of exchange and expected to retain a stable value by reference to other forms of capital". Note that "The Commission expressly refrains from using the term 'stablecoins', considering it to be a 'marketing concept' rather than a term that accurately reflects the nature of the crypto-assets in question", *see infra*, II, Title 2, 2.4.

[751] *Op. cit*, art. 3 and 1. Background to the proposal, 3. 4. Budgetary impact: "token referring to an asset or assets: a type of crypto-asset that aims to retain a stable value by referring to the value of several fiat currencies that are legal tender, to one or more commodities or to one or more crypto-assets, or to a combination of such assets; e-money token: a type of crypto-asset whose main purpose is to be used as a medium of exchange and which aims to retain a stable value by reference to the value of a fiat currency that is legal tender", available at the following address

stablecoins of "*significant importance*", i.e. those that are widely accessible and intended for the public. To date, it would appear that the majority of stablecoins on the market (USDT, Tether)[752] fall into this second category within the meaning of the Regulations. In this respect, MiCA imposes issuance ceilings and certain non-exhaustive conditions for the issuance of these two types of stablecoin[753] . Some of the standard rules include the obligation to notify the EBA of the planned issuance of a stablecoin by means of a "white paper", the need to be legally domiciled in the European Union in order to subject all foreign players to EU rules, and the requirement to set aside substantial reserves to prevent any risk of insolvency. However, these rules do not apply to the few "*algorithmic stablecoins*"[754] , which are highly decentralized thanks to the use and interlocking of smart contracts. However, as the European legislator does not recognize this partially decentralized nature, these algorithmic stablecoins do not benefit from the exemptions also granted to Decentralized Finance Solutions (DeFi) and, in part, to insignificant NFTs. Ultimately, the issuer of a stablecoin will be obliged to reimburse any user at any time, free of charge, in accordance with MiCA provisions. In this respect, the EBA may sanction issuers of tokens referring to assets of significant importance[755] with fines and/or periodic penalty payments in the event of non-compliance with certain provisions (*see* Appendix V of these Regulations).

On June 30, 2022, the consultation, negotiation and discussion phase lasting over two years came to an end for this proposal to adopt the MiCA Regulation[756] . It is expected to be published in the OJEU i n mid-2023, and to come into force 15 to 18 months later, i.e. between

[752] CoinMarketCap, "Top Stablecoin Tokens by Market Capitalization", accessed October 24, 2022. See the real-time list of *stablecoin tokens* available on the cryptoasset market at
[753] See *infra*, II, Title 2, 2.4
[754] CANT Tim, RICE Bradley, "10 things you need to know about MiCA: Europe's proposals for regulating crypto assets." 2020, in *www.ashurst.Com,* "'Algorithmic stablecoins' should not be considered 'electronic money tokens', although they may be subject to the requirements applicable to cryptoassets more generally. Algorithmic stablecoins are designated as those that aim to maintain a stable value, via protocols, which provide for the supply of these cryptoassets to increase or decrease in response to changes in demand.", available online, *see* also Part II, Title 2, 2.4
[755] *Ibid.* MiCA. Title III, Chapter 5, art. 39, "the criteria to be applied by the EBA to determine whether an asset-based token is of significant importance. These criteria are: the size of the customer base of the promoters of asset-based tokens, the value of these tokens or their market capitalization, the number and value of transactions, the size of the asset pool, the importance of the issuers' cross-border activities and the interconnection with the financial system. Article 39 also empowers the Commission to adopt a delegated act in order to specify the circumstances in which and the thresholds above which an issuer of tokens referring to assets will be considered to be of significant importance".
[756] European Parliament News, "Cryptocurrencies in the EU: deal struck between Parliament and Council", 2022, available online at

September and December 2024. It should be noted that an additional transitional period of 18 months is granted to players who have already obtained PSAN registration or approval, enabling them to continue providing their services to the French public while awaiting approval and the European "PSCA" passport referred to in the MiCA visa. Finally, with this Regulation, the European Union will become a pioneer in setting up a comprehensive regulatory framework dedicated to crypto-assets and their ecosystem of providers. MiCA also paves the way for a number of other texts currently being drafted for the aforementioned applications of 3.0 technologies[757] . Indeed, there is provision for a review clause in the Regulation for the purpose of considering whether new complementary provisions[758] were necessary, which would be welcome given the context previously outlined. As with the RGPD, these rules establish European standards and will probably spin off numerous international regulations. While the drafting and then the amendments to the MiCA Regulation were confronted with several political attempts to economically and legally destabilize crypto-economy players, its final adoption will undeniably provide a foundation of confidence for consumers as well as players in these ecosystems. Nonetheless, once the Regulation comes into force, one of its consequences will be the establishment of countless multilateral information exchanges between exchange platforms and national or international supervisory institutions. The transit of this information entails a risk of data leakage, as there is no provision for an independent audit of each PSCA's IT security systems. Only their responsibility is invoked, which is insufficient, as not all providers have equivalent levels of IT security, depending on the IT culture of each member state, as mentioned in the previous sections. It is here, therefore, that the decentralized digital identity[759] seems unavoidable in order to meet these information transmission obligations, which are also provided for in the LCB-FT Regulation[760] .

2.5.2 Amendment to the Transfer of Fund Regulation (TFR)

According to some lawyers and players in the crypto-asset sector[761] , a second attempt at relatively excessive legal regulation of this sector has been identified alongside the MiCA Regulation, as stemming from political motivations similar to those mentioned above. The *anti-money laundering package*[762] of

[757] A second version of MiCA, dubbed "*MiCA-2*", will provide a framework for *NFTs* and *decentralized finance* (*DeFi*).
[758] *Ibid.* MiCA. 5. Other elements. Available at the following address, It is important to note that the Commission may adopt delegated acts in order to clarify certain technical elements of the definitions and adapt them to market and technological developments.
[759] See *below*, II, Title I, Chap. 1
[760] V, next part.
[761] *Ibid.* FLEURET Faustine, Grand Angle Crypto, "Réglementation kaMICAze en Europe?", 2022, "Les derniers débats [MiCa et TFR concernant la lutte contre la PoW] sont assez inquiétants", available at,
[762] EC, Anti-money laundering and countering the financing of terrorism legislative package. Accessed on October 26, 2022, at the following address

the European Commission includes a revision of the Transfer of Funds Regulation ("*TFR*")[763] which extends to PSCAs the traditional obligation of financial institutions to accompany transfers of funds and information on the beneficial owners of funds in crypto-assets. On April 31, 2022 certain proposed amendments (article 15[764] and article 16[765]) to this Regulation were adopted. The TFR will apply as soon as MiCA is implemented, i.e. within the same timeframe as from its publication in the OJEU. Some of these new articles relating to PSCAs and crypto-assets are examined in this section. On July 20, 2021[766] , the Commission adopted an anti-money laundering and combating the financing of terrorism (AML/CFT) legislative package, including a proposal to revise Regulation 2015/847/EU[767] on information accompanying transfers of funds including with crypto-assets. Since 2021, Interpol[768] , as well as the European Commission with the present proposal to amend this Regulation[769] , believes that the pseudo-anonymity and global reach of crypto-assets lead to risks of use for criminal purposes as mentioned above. The European regulatory framework to prevent money laundering and terrorist financing, which now encompasses crypto-assets, is based on several recommendations dating back to 2012 (n°15[770] and 16)[771][772] proposed and updated by the Financial Action Task Force (FATF). This "*Travel* [of Funds] *Rule*"[773] concerns mandatory minimum information that must accompany a financial transfer, in this case in crypto-assets. These

[763] This proposal takes as its starting point and amends the existing Regulation (EU) 2015/847 of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, as amended by Regulation (EU) 2019/2175 of 18 December 2019.V. Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast), available at.

[764] Relating to PSCA beneficiaries and the new due diligence obligations for any beneficiary of crypto-assets.

[765] Relating to asset-issuing and registered (MiCA) PSCAs, which are subject to new, enhanced information-gathering obligations when sending funds to *non-hosted digital asset portfolios*, see following pages. *Op. cit.* According to a March 24, 2023 study, 80% of crypto-asset holders host and store them within a platform and with a trusted third party, and only 30% hold them cryptographically on one or more nonhosted wallets. in *CoinGeco*, "Where People Store Their Crypto, Post-FTX Collapse", 2023, available at.

[766] CE, Press corner, 2021, consulted on April 5, 2022, at the following address

[767] Regulation (EU) 2015/847 of May 20, 2015 on information accompanying transfers of funds (TFR) and repealing Regulation (EC) No. 1781/2006.

[768] EUROPL, "Europol's Internet Organised Crime Threat Assessment", p.15, available at

[769] *Op. cit*, TFR, Explanatory Memorandum, 1. Context of the proposal, "Given that virtual asset transfers are accompanied by money laundering and terrorist financing risks similar to those surrounding electronic fund transfers, it is to requirements of the same nature that they should be subject, and it therefore seems logical to use the same legislative instrument to address these common problems".

[770] EC, Interpretative Note to FATF Recommendation 15: "Countries should ensure that [PSCA] issuers obtain and hold the required and accurate originator information as well as the required beneficiary information for virtual asset transfers, submit the above information to the [PSCA] or the beneficiary's financial institution (if applicable) immediately and securely, and make it available to the appropriate authorities upon request" and that "the [PSCA] beneficiaries obtain and hold the required originator information and the required and accurate beneficiary information for virtual asset transfers, and make it available to the appropriate authorities upon request. "Available at the following address

[771] FATF, FATF Recommendation 16, 2021, "updated guidance for a risk-based approach - virtual assets and virtual asset service providers". p.58, available at the following address

[772] *Ibid*. FATF Recommendations.

[773] *Op. cit*, TFR, 3. Results of ex post evaluations, stakeholder consultations and impact assessments, TFR, art. 4, available at the following address, "transfers of funds for which the payment service provider of the payee is established outside the Union, the amount of which does not exceed EUR 1,000 and which do not appear to be linked to other transfers of funds the amount of which, cumulated with that of the transfer in question, exceeds EUR 1,000, shall be accompanied by at least the following information: a) the names of the originator and the beneficiary of the funds; and b) the payment account numbers of the originator and the beneficiary of the funds or the unique transaction identifier".

transactions are carried out between virtual wallets[774] containing crypto-assets, being designated as belonging to PSCAs (legal entities) or individuals (natural persons)[775] . This Travel Rule enshrines this principle of mandatory identification of crypto-asset beneficiaries, as soon as a crypto-financial transfer of an amount greater than 1,000 euros is involved[776] . In practice, this means that certain mandatory information (surname, first name, address, unique identifier) of the actual beneficiary of the funds will be systematically associated with this type of crypto transaction. The broadening of this recommendation is intended to enable information to be shared between, on the one hand, PSCAs subject to the LCB-FT regime, and, on the other, the said beneficiaries of crypto-asset transactions. Although this recommendation proposed by the FATF is not mandatory in nature, since the FATF issues non-coercive recommendations, it is clear that many developed countries, including France, systematically transpose these recommendations into domestic law for strict application by the AMF or the ACPR.

To recontextualize, on February 9, 2022, two EU economic policy committees (LIBE and ECON)[777] made up of two factions of the European Parliament (The Greens[778] and the European Conservatives and Reformists[779]) presented a draft regulation aimed at combating money laundering and the financing of terrorism using crypto-assets. This draft amendment follows the FATF's official and decisive advice. In its version consolidated by a vote of these committees, it aims to apply an "*Enhanced Travel Rule*"[780] , initially conceived as an effective traceability and control tool for centralized IT and social systems, such as those of financial institutions. The transposition of this Rule of Travel to decentralized ecosystems and technologies seems inappropriate, as the following comments suggest. In fact, the two initial proposals - the aforementioned Enhanced Travel Rule and the reduction in the tolerance threshold (below) - were designed to bring the crypto-economy into line with the same standards as traditional financial networks, such as SWIFT. In principle, this rule would therefore be applicable for every crypto-transfer in excess of €1,000[781] , with PSCAs required to inform the competent authorities in order to register this minimum identification information considered essential for LCB-FT. It is

[774] See *infra*, II, Title 1, 1.3.1.3.
[775] *Op. cit*, TFR, see recitals and definitions (12) to (20): "'wallet address' means an account number maintained by a cryptoasset service provider or an alphanumeric code relating to a wallet on a blockchain"; "'transfer of cryptoassets between individuals' means a transaction between natural persons acting, as consumers, for purposes other than commercial or professional, without recourse to or intervention by a cryptoasset service provider or another reporting entity", etc.
[776] *Op. cit*, TFR, art. 5.
[777] On November 25, the case was assigned jointly to LIBE and ECON, with Ernest Urtasun acting as rapporteur for the ECON Commission and Assita Kanko for the LIBE Commission.
[778] Wikipedia contributors. "Green Group/European Free Alliance", 2022, available at
[779] Wikipedia contributors. "European Conservatives and Reformists", 2022, available at
[780] Of which the amendments specifically applicable to crypto-assets are stricter than those concerning the banking and financial sector.
[781] Art. 4 and 5 of the TFR Regulations, available at the following address

pointed out that on March 31, 2022[782] , the EU Commission, wishing to go beyond this tolerance threshold of 1,000 euros below which the FATF considers an exemption from identification to be possible, attempted to reinforce this identification by trying to abolish it. Had this manifestly disproportionate attempt been successful, it would have meant the collection and verification of countless personal data for every transfer of crypto-assets within the EU, from as little as one euro. Similarly, the same Commission wanted to introduce the identification of all non-hosted[783] crypto-asset wallets (essential for any P2P transfer)[784] , an obligation also disproportionate to the AML/CFT objectives pursued, as it is not covered by the FATF recommendations. Ultimately, this attempt to require identification of every P2P transfer between individuals (a case without PSCA), *was* rejected, again thanks to the efforts of lobby 3.0 players led by the Association pour le dévelopement des actifs numériques (ADAN). According to Stéphane Berger, one of the members of the European Parliament and rapporteur for the MiCA Regulation: "*implementing the* (...) *rules of the TRF would be like asking for a passport for a €20 cash payment when shopping at the Supermarket*"[785] . Indeed, ahead of the European Parliament's vote to confirm these amendments, many (re)well-known players in the[786] ecosystem wrote an open letter in April 2022 to European governments[787] regarding the risks of such proposals, while some French players more radically announced that they were leaving the national territory in the face of this second attempt at political-legal restrictions targeting their sector and their activities[788] .

Finally, the compulsory and reinforced identification from the first euro of the transfer was repealed and replaced by another amendment, the legal and IT effectiveness of which is subject to change.

[782] Draft report on the proposal for a regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets, see in particular amendments 68 on art. 18a, 15 on art. 27b and 52 on art. 14 and 5, available at the following address

[783] A *non-hosted crypto-asset wallet*, also known as an "*unhosted wallet*" or "*cold wallet*" in English, enables a user to maintain a crypto-asset balance alone outside of any trusted third party (exchange platforms, so-called "In fact, crypto-assets are stored on one or more "hosted *wallets"* or "*hot wallets"*, using their own private cryptographic key, just as if they had banknotes in their own wallet. According to a March 24, 2023 study, 80% of crypto-asset holders host and store them with a platform and a trusted third party, and only 30% hold them cryptographically on one or more non-hosted wallets, *op.cit.* "Where People Store Their Crypto, Post-FTX Collapse", 2023, available at.

[784] V*, supra,* I, Title 1, 2.3.1.1.c

[785] BERGER Stephan, "EU Parliament's MiCA Rapporteur, talks about crypto regulation in the EU", 2022, in *Cryptolaw* [Video]. YouTube

[786] Created in 2019, ADAN is a trade association that federates players in the crypto-asset and blockchain sector to establish France and Europe as innovators in this space. ADAN has played a key role in defining the various regulatory frameworks for crypto-assets in France. Among other things, its position as a trade association enables it to educate legislators on the many innovations and challenges of the crypto-asset ecosystem.

[787] RAYMOND Gregory, "Exclusif MiCA: l'industrie crypto interpelle les gouvernements européens", 2022, in www.thebigwhale.io. Accessed May 3, 2022, at the following address

[788] PLANCADE Jean, "Durcissement régulatoire dans l'UE - L'exode de la crypto européenne vers la Suisse s'accélère", 2022, in *Bilan*, available at the following address. Among them, entrepreneur Sébastien Gouspillou, president of *BigBlock Datacenter*, who has announced that he is continuing to raise $200 million in the Swiss canton of Neuchâtel, at the expense of France.

interpretation[789] . While, in principle, any transfer of less than €1,000 does not oblige a PSCA to identify the beneficial owner of the funds as mentioned, there is an exception which overturns this rule, i.e. when multiple small-value transactions are carried out, the total amount of which exceeds the €1,000 limit (which triggers the identification obligation). In fact, this amount and ceiling trigger identification within three days at the latest, by the PSCAs concerned. This amount of €1,000 is extremely low when compared to the median amount of €5,000 held by French crypto-investors according to a 2021 survey "*the median crypto portfolio value is around €5,000, while 29% of those surveyed manage between €5,000 and €25,000, 6.4% manage more than €100,000*"[790] . Consequently, this exemption from identification below €1,000 will not affect the majority of crypto-asset users in the medium term, who may hold larger amounts in the future. This finding thus seems to distance the crypto-asset ecosystem and its users from their initial desire to use[791] peer-to-peer electronic cash that respects their privacy. By way of comparison, cash does not impose such strict, automated identification requirements. Because the temporality of this 1,000-euro threshold is not defined in the TFR, this means that all Internet users with more than 1,000 euros in crypto-assets will necessarily be identified and their funds monitored, a principle with the long-term effect of recentralizing crypto-assets, which will then be censurable at the slightest suspicion of non-compliance (proven or not). For some observers and specialists involved in this 3.0 ecosystem, including legal experts, this risks introducing a form of active and generalized surveillance that could run counter to the free circulation of financial flows within the EU[792] . With regard to the possibility of autonomously holding a portfolio of non-hosted crypto-assets[793] , this is still considered by many users to be the safest way of storing and holding them cryptographically, compared to centralized solutions dependent on PSCA, which are regularly prey to targeted computer attacks or massive scams. In this respect, it is argued that preventing or hindering the use of these crypto-currency wallets (P2P and non-hosted) is tantamount to preventing or hindering certain freedoms associated with crypto-assets (freedom of ownership, etc.).

[789] *Op. cit,* TFR, Section 2, art. 7, 4: "For transfers of funds which do not exceed EUR 1,000 and which do not appear to be linked to other transfers of funds which, together with the transfer in question, exceed EUR 1,000, the payment service provider of the payee is not obliged to check the accuracy of the information on the payee.
[790] ARMANDET Pauline, "French crypto-investors are almost exclusively men", 2022, in *agefi.fr*
[791] *Op. cit. "*Bitcoin: A Peer-to-Peer Electronic Cash System", available at
[792] European Parliament, "The free movement of capital", Fact sheets on the European Union, "All restrictions on the movement of capital between Member States and between Member States and third countries must be lifted, save in exceptional circumstances. The free movement of capital is the cornerstone of the single market and complements the other three freedoms. It also contributes to economic growth [...]", 2021, consulted online
[793] For a few hundred euros, you can set up your own cryto-asset management and storage system, right in your own home. For more information, see the Umbrel solution. *Op. cit.* According to a March 24, 2023 study, 80% of crypto-asset holders host and store them with a trusted platform and third party, and only 30% hold them cryptographically on one or more non-hosted wallets. Available at

[794] , freedom of communication[795] , freedom of movement of capital). The new version of the TFR Regulation will therefore have the effect of massively identifying all users of crypto-assets, while at the same time encouraging the use of wallets hosted by PSCAs, which the history of this sector demonstrates to be less secure for less sophisticated users. This informatically undesirable legal effect thus forms a paradox to the detriment of the actual beneficiaries of crypto-assets[796] . In addition to the above, ADAN has identified and highlighted a number of dangers concerning the impact of the proposed amendments to the TFR Regulation:

(i) Dangers concerning the protection of personal data, individual privacy and European digital sovereignty. The *Travel Rule* must in principle respect a balance between an essential LCB-FT[797] , and protecting the privacy of crypto-asset users, the majority of whom are acting in good faith (few transactions actually involve signs of money laundering according to specialized companies that collaborate with Interpol[798]). From now on, it's vital that SCSPs comply with the RGPD and only transfer information about their users if the protection of this data is ensured, which opens up - as with MiCA - the field for the decentralized identity market to efficiently meet this new requirement[799] which some SCSPs rightly consider complex to implement. To date, the PSCAs have not yet put in place technical solutions that meet the TFR requirements for accompanying personal data transfers. To remedy this shortcoming, the use of decentralized identity solutions is recommended to guarantee reliable identification and avoid certain risks linked to RGPD non-compliance, personal data theft, identity theft, among others. Although these 3.0 solutions are particularly well suited to the constraints imposed by these proposals

[794] V*, infra*, II, Title 1, 2.2.6
[795] V*, infra*, II, Title 1, 2.2, *see* also Appendix 3, Focus 6.
[796] Even if a user is protected in the event of loss of his assets due to the negligence of an asset custody service provider (ACSP), it is often difficult and laborious to prove this negligence, as illustrated by the Mt. Gox platform case (ACSP) which lasted more than seven years before the courts. V. ICHBIAH Daniel, "Les victimes du piratage de Mt. Gox dédommagés 7 ans après la disparition de leurs Bitcoins", 2021, in *Futura-sciences.com*, available at the following address
[797] EC. European Parliament, "Crypto-assets: new rules to stop illicit flows in the EU", 2022, accessed at
[798] Leading anti-money laundering firm *Chainalysis* found that only 0.15% of crypto-currency transactions in 2021 involved an element of criminality, "Money laundering accounted for only 0.05% of total crypto-currency transaction volume in 2021", "The 2022 Crypto Crime Report", 2022, in *chainalysis.com*, p.5.
[799] *Op. cit*, TFR, "The implementation of the 'travel rule' introduces [...], new specific requirements that oblige them [PSCA] to obtain, retain and share the required and accurate information on users of virtual asset transfers and to make it available at the request of the relevant authorities. Such obligations raise various technical difficulties, due to the need for virtual asset service providers to develop technological solutions and protocols to collect and share such information both among themselves and with the competent authorities. [...] it involves the introduction of new FATF international standards which must be applied simultaneously in several countries around the world [...]", available at the following address

amendments, it is important to ensure that their IT implementation is not dependent on foreign players, but rather on European ones.

(ii) Risks to European economic competitiveness. In terms of economic sovereignty, it could be risky to mandate foreign players, particularly platforms headquartered outside the EU, to automatically transmit such sensitive and high value-added civil identity information (as is already the case for the majority of social networks, which are Chinese or American, as previously noted). As such, a foreign PSCA - often subject to less restrictive legislation - could exploit this data for its own strategic or economic interests, which is why end-to-end encryption using decentralized identity computing standards is recommended. As some PSCAs[800] apprehend, their competitiveness could be reduced by the obligation to implement this enhanced travel rule requirement concerning the movement of funds in crypto-assets. Competition to attract international players is intensifying, as evidenced by a recent announcement by the UK government to introduce flexible and advantageous regulations for these players[801] , following the example of the USA[802] .

Ultimately, in the light of articles 263 and 264 of the TFEU[803] , and articles 7 and 8 concerning the free movement of capital protected by the EU Charter of Fundamental Rights[804] , the following question needs to be asked: are the infringements of these fundamental freedoms proportionate and justified on the simple grounds of combating money laundering and the financing of terrorism? The collection of personal data on the beneficiaries of crypto-asset funds could remain declaratory and carried out on a case-by-case basis, and not be based on a generalized principle of suspicion, which is certainly more effective, but partially disproportionate or even liberticidal in relation to the objective pursued (on the one hand, creating "*honeypot"* institutions for hackers, and on the other, contributing to a form of mass surveillance of taxpayers[805]). In reality, the legislator needs to strike a genuine balance between AML/CFT procedures and certain fundamental rights

---

[800] *Ibid*. "some representatives of virtual asset service providers in the EU27 have argued that the lack of a standardized, free and open global technical solution for the travel rule could result in the exclusion of smaller players from the cryptoasset market, with only the larger market players having the means to comply with the rules." [801] HM Treasury, "Government sets out plan to make UK a global cryptoasset technology hub", in *GOV.UK*, accessed April 4, 2022, at.

[802] The White House, "Fact sheet: President Biden to sign executive order on ensuring responsible development of digital assets", 2022, consulted on April 12, 2022, at the following address

[803] Art. 263 of the Treaty on the Functioning of the EU (also known as the Treaty of Rome): "The Court of Justice of the EU shall review the legality of legislative acts, acts of the Council, of the Commission and of acts of the European Parliament intended to produce legal effects vis-à-vis third parties (...)" and v. art. 264 "If the action is well founded, the Court of Justice of the European Union shall declare the contested act null and void (...)".

[804] Art. 7 of the Treaty on the Functioning of the EU: "Everyone has the right to respect for his private and family life and for his communications"; see also art. 8 "Everyone has the right to the protection of personal data concerning him".
".

[805] SEZNEC Erwan, "Comment Bercy a tenté d'accéder à nos données bancaires", September 28, 2022, in *Le Point*, available online.

(protection of users' personal data and their right to privacy), a complex process where political lobbying and a lack of technical and commercial knowledge go hand in hand. In practice, crypto-assets are an inefficient and unprivileged vector for laundering the fruits of illegal activities. Indeed, there is a permanent record of every transaction on these public blockchains, which are currently analyzed and monitored on a daily basis by specialized companies. In 2022, according to the "Chainanalysis Crypto Crime Report"[806] , the share of illicit activities in the volume of crypto-asset transactions has never been so low (representing only around 0.15
% of all identified transactions). As these tools for analyzing public blockchains and the number of investigators increase, criminals are gradually ruling out this vector as a means of opacifying the illicit origin of their funds. Note that, according to Europol, around 1% of the EU's annual gross domestic product is identified as being involved in suspicious financial activity, with crypto-assets therefore representing only a tiny fraction of this figure (~0.15%), demonstrating the questionable proportionality of this enhanced Travel Rule imposed by the forthcoming amendment to the TFR Regulation.

2.6 Blockchain and decentralized identity with regard to intellectual property

The dissemination of progress and knowledge is one of the foundations of the development of intellectual property, as emphasized by several researchers at the Institut Mines-Telecom: "*the objectives of intellectual property protection* (...) *consist in granting a temporary monopoly to the inventor for the industrial and commercial exploitation of his invention, in exchange for which the inventor is obliged to disclose the principles of his invention, thus promoting the dissemination of technical knowledge in the industrial fabric*"[807] . In this section, blockchain technologies and decentralized identity solutions, examined in the second part of this study, are mainly approached from the angle of intellectual property and trademark, patent and software copyright law[808] . The following table proposes to introduce and identify the relationships between the notion of intellectual property (IP) in law and that of 3.0 applications (usages) in IT:

[806] Chainalysis, "Crypto Crime Report", *op. cit.* available at
[807] VALERIAN François, COMBY Gérard, KAPPELMANN Alexia, GIMON Magali, et al. " Annales des mines n°18 sur les enjeux numériques : propriété et gouvernance du numérique", quarterly series - N°18 - June 2022, Institut Mines-Télécom, p.72, available at
[808] Software can be defined as a set of programs designed to perform a particular operation on a computer. Software is protected by copyright under article L.112-2 of the French Intellectual Property Code, which states: "(...) 13° Software, including preparatory design material (...)".

Does IP apply to 3.0 technologies?		
Trademark law	Patent law (Software)	Copyright (Software and others)
Yes	Yes	Yes

Software copyright has its origins in the necessary protection of new technologies and their competitive and commercial needs. With the advent of blockchain technology and its constant innovation, particularly in terms of decentralized digital identity, new technical possibilities are emerging, creating new social opportunities, but also legal challenges. In 2020, the international context is such that China and the United States were at the top of the country breakdown of the world's top 100 companies filing patent applications relating to blockchain technologies[809] . France does not feature in this ranking, perhaps due to an initially less accommodating visibility or regulatory constraints for innovation compared to other jurisdictions, as studied previously. It should be noted, however, that the research tax credit (CIR) and the tax credit for competitiveness and employment (CICE), from which a very large number of companies in the French sector benefit, tend to qualify this observation. As mentioned above, the ecosystem of crypto-assets and blockchain technology was initially created in an open and transparent way, with "open source" computer programs[810] , as developed by communities of developers. Apprehending a decentralized service raises the question of who owns intellectual property rights, and the extent of these rights inherent in these new ecosystems (patents, trademarks or copyrights). Software is mostly protected by the copyright attached to computer programs, as the latter are created and maintained by individuals operating within the framework of Web 3.0 and its conceptual perimeter containing multiple technological bricks (AEC, DAO, blockchain protocols, etc.). Intellectual property applies here, while the trusted third parties who interact with them have an extended license of use, generally provided by default by sites such as GitHub, hosting a large proportion of these computer programs[811] . In terms of copyright, blockchain technology offers many advantages, such as facilitating proof of prior rights acquisition, disclosure or time-stamping of works or digital evidence[812] . The traceability and integrity supposedly offered by a blockchain make it possible to trace every stage in the creation process of a literary or artistic work, which

[809] Statista, "Global blockchain patents major applicants; country distribution 2020", accessed on March 7, 2022, at.
[810] V*, infra*, II, Title 1, 1.5.3.1
[811] Platform available at the following address
[812] See Part I, Title 2, 2.8 *below.*

is particularly relevant in the case of multiple collaborations, especially for co-authorship schemes[813] . In this context, the use of a public blockchain can offer micropayments proportional to the assignment of certain economic rights associated with a work, such as a musical work, for both the author and the beneficiary of the work. In August 2022, the European Commission announced that it will develop a system that uses blockchain and smart contracts[814] . The European Union's World Intellectual Property Organization (WIPO) plans to develop a system enabling intellectual property owners to create product-backed AECs to prove authenticity. To use this blockchain-based tracking system, IP owners will need to be registered as approved signatories. The European Intellectual Property Office aims to have an operational system by the end of 2023. Yet blockchain technology does not prevent certain common and proven[815] infringements, such as counterfeiting or copying software without respecting the moral rights of its authors and developers. Thus, it is conceivable that the growing adoption of these applications, which are often both centralized and decentralized (DAO, DeFi, AEC), will inevitably lead to litigation concerning the infringement of intellectual property rights. What's more, while blockchain protocols are open source[816] , some crypto-asset-based services developed by providers and companies nevertheless remain the exclusive, closed property of these commercial entities. As a result, it can be seen that while public blockchains are open source from design and access through to (re)use, their social ecosystems are becoming progressively less open[817] , as with the hybrid and especially private blockchains studied earlier. In particular, public blockchains linked to self-sovereign digital identity solutions (INAS)[818] may in the future be a source of concern and complexity, not least because of the publicity and imuability of their digital transactions. Indeed, infringements of copyrights, trademark licenses, patents or designs are already flourishing for the most decentralized applications of these technologies. For example, many blockchain applications advocate end-to-end decentralization, i.e. the inability of a third party to claim a right to the information deployed by them. This is notably the case with the "Ethereum Name Service - ENS"[819] , which provides decentralized domain names linked to crypto wallets.

---

[813] Art. L.113-3 of the French Intellectual Property Code, in the version in force since July 3, 1992, states: "A work of joint authorship is the joint property of the co-authors. The co-authors must exercise their rights by mutual agreement. In the event of disagreement, it is for the civil court to rule (...)".

[814] WIPO (contributions prepared by the European Union and the Tencent Group), "Advisory Committee on Enforcement - fifteenth session - new technologies in ip enforcement", WIPO/ACE/15/10, 2022, available at, see also *supra*, Part I, Title 1, 2.3.1.1.d

[815] MALONEY Conor, "Researchers Allege Tron Plagiarized Code from other Crypto Projects", 2022, in *Yahoo Finance*, available at.

[816] See *infra*, II, Title 1, 1.5.3.1.

[817] V. Appendix 7 and Appendix 6, Focus 3.

[818] See *infra*, II, Title 1, 2.2.1.

[819] For more information, visit the *decentralized domain name* creation and management service *at the* following address

active (to facilitate identification and crypto-payments between websites and their owners). While in theory, the operation of these domain names is decentralized, in practice many of their technical and legal components remain centralized[820] . However, the fact that certain protocols are still partially decentralized leads to administrative and IT complications concerning the identification of the legal entities and individuals responsible, which sometimes makes legal action impossible. By browsing the ENS application mentioned at[821] , we can see that it enabled an (anonymous) user to register the domain name "*banquedefrance.eth*", most probably without the authorization of this institution (as holder of the "Banque de France" trademark registered with the INPI). This is probably a case of counterfeiting (admittedly without any commercial use to date), one of many that remain undetected due to the modest size of this service (~800,000 ENS registered in 2022).

In addition, it should be noted that the regulation of PSCAs under the MiCA and TFR Regulations, studied in advance, could consequently reduce the number of infringements of these intellectual property rights. This is due to the fact that these infringements will be linked to crypto-assets whose owners will be identified, thus facilitating the identification of those responsible in the event of a PSCA being used to transit - as an infringer - these domain names and their associated funds. A distinction needs to be made between pre-existing intellectual property components and those newly generated as part of a decentralized application. This first distinction must be made with regard to the degree of decentralization of each 3.0 application. The responsibility for integrating open-source or third-party software must also be taken into account at the outset of any development activity. In this respect, this study suggests that within private and hybrid blockchains, it is commonly accepted that intellectual property should be contractually framed prior to any IT development[822] . Thus, two considerations and certain compromises are necessary within these consortia of players:

(i) In principle, joint ownership (within the meaning of the French Civil Code) should be avoided, given the constantly evolving nature of software development within these 3.0 consortiums.

(ii) A system of co-ownership in which all consortium members have prior knowledge and rights is to be preferred, with each member free to supply or not certain technological bricks to the consortium, and to benefit from licenses to use them where appropriate.

[820] Notably through a foundation registered in the Cayman Islands, or through a decentralized organization (DAO) whose management and distribution of dedicated digital tokens (called "ENS") remain under the influence of the said foundation and its owners.
[821] To view this probable trademark infringement online, visit the following address consulted on 28/08/2021.
[822] Software, even standard software, is an intellectual work which, if original, is protected by copyright (reproduction, use, adaptation, representation). The use of software can take several forms, depending on the type of license contract.

In the final analysis, it appears that blockchain technology and, more broadly, the Web 3.0 technological building blocks of which it is composed, fit seamlessly into the legal framework(s) of intellectual property rights, certainly to the benefit of the developers of these 3.0 IT solutions, but which paradoxically remain constantly evolving, and sometimes particularly open and decentralized, i.e. partially defying intellectual property law.

2.7 Legal professions and decentralized technologies

Jurists represent a "*social and intellectual caste*"[823] in the same way that technophiles, like crypto-anarchists, have theirs[824] . The Internet and its many technologies, both old and new, are no exception to this social and community principle, which lawyers are gradually coming to grips with in the digital world. Decentralized technologies are having a growing impact on the world of law and related professions, particularly in view of the adoption of crypto-assets. Between 2016 and 2021, many lawyers and notaries were worried that their role and profession would disappear in a wave of IT decentralization. The opposition between the techno-anarchists of decentralization on the one hand, and the administrative and intellectual centralization of lawyers on the other, is indeed intrinsic, as some authors suggest "*we can see at what level of depth the possible rivalry between law and blockchain lies: the latter claims to do in a more scientific and unfalsifiable way the same work vis-à-vis transactions in the ordinary world as that performed by law, i.e. to qualify and therefore, ipso facto, to judge*"[825] . However, the postulate of an entirely algorithmic and decentralized law only seems utopian in view of the construction of our societies, where social decentralization generally seems to have little room and little chance of being introduced. Faced with this innate need for trust and this social and behavioral reality, the limits of 3.0 technologies become apparent. Indeed, and paradoxically, building bridges between these decentralized solutions and the centralized players in our society requires more the intervention of a legal professional, i.e. a trusted third party whose identity and responsibility are clearly established for carrying out legal transactions (civil, contractual, fiscal and financial, real estate, judicial). According to journalist and author Marc Bousquet: "*blockchains are forcing us to reinvent the professions of forensic scientist and jurist, while coders are called upon to make law - more or less consciously.*"[826] . Finally, it appears that any decentralized service (whatever its degree/scale of decentralization)

---

[823] *Op. cit.* LASSEGUE Jean, GARAPON Antoine, " Justice digitale ", pp.102-103, " Les avocats ont l'habitude de croiser le fer avec les notaires, les avoués, les experts-comptables, les juristes d'entreprise, mais à chaque fois, tous restent dans la grande famille des juristes ".
[824] *Op. cit.* GIRARD, Guillaume, "A Tale of Chaos vs Order: The ideological war between Bitcoin and Ethereum doesn't need to happen", Medium, accessed June 21, 2022, at the following address, *see* also Appendix 3 and 6.
[825] *Op. cit*, "Digital justice", p.140. Kindle ed.
[826] *Op. cit,* BOUSQUET Marc, "Tout savoir sur le Bitcoin et les cryptomonnaies", Dossiers Science Hors-Série, in ed. *du Sens*, ISSN: 2802-1843, November 2022, p. 41.

cannot do without the *ante-* or *post-intervention of* a legal professional, all the more so in view of the recentralization that the application of the MiCA and TFR regulations will entail. This can also be explained by history, experience, the guarantee of the rights of litigants and the quality of the legal profession in our society. While the lawyer's neutral point of view undeniably enables him to stand back from the technical object in question, it sometimes distances him from its proper understanding and therefore from its legal apprehension[827] . Thus, a subtle balance between technical acculturation of jurists and stepping back (education)[828] will be necessary if more and more 'augmented' jurists are to emerge in the future. Any decentralized code must implement a system of governance (IT and social): this is the IT rule that inherently applies to blockchains, depending on its extrapolation and legal acceptance. For example, once the various technical and legal applications of blockchain are understood in the minds of legal practitioners, they need to consider the potential tensions between current intellectual property law and personal data protection law as applied to Web 3.0. Indeed, the laws and rules applicable in the jurisdictions concerned are essential knowledge for 3.0 professionals, not least in order to understand restrictions on, for illustration, the content, formats and storage location of blockchain information and evidence. Faced with these sometimes radical developments, as with public blockchains and crypto-assets, the world of law and its practitioners sometimes find that the substance (legislative) and form (business) of their practices are evolving, without always understanding or accepting the origins and reasons for this. As a result, the legislative body[829] tends to want to frame any unidentified legal object, sometimes with the support of certain legal experts[830] , but also sometimes with a lack of knowledge and consequent capacity for technological anticipation. In reality, open minds and fields of expertise seem intimately linked. Consequently, it seems important for lawyers to collaborate with developers to understand the legal effects of decentralized programs and their relationship with every branch of law and every piece of legislation. In practice, blockchain will impact legal professionals, as is already the case for compliance directors (KYC, LCB-FT). As such, the role of certain legal professionals will be to re-identify certain beneficiaries and holders of crypto-assets, in line with the introduction of the new regulatory framework mentioned above. Mainly due to its financial origin from Bitcoin[831] , the main current use cases remain financial. Nevertheless, many others are already proving their worth, such as the use case of blockchain certification (of

[827] *Op. cit.* JEAN Aurélie, "Les algorithmes font-ils la loi?", "[...]es prochains textes ne pourront être articulés correctement que s'ils sont pensés et construits sur la base de connaissances et de savoirs scientifiques et technologiques approfondis", reading position in the book: 10%.
[828] See *infra*, II, Title 1, 1.5.3.2.
[829] GAYTE Aurore, "Les sénateurs ne comprendraient rien aux cryptos et une sénatrice veut changer ça", 2022, in *Numerama*, article available at.
[830] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, "L'identité numérique; quelle définition pour quelle protection?", 2020, p.162, "The legal apprehension of the digital world is a source of undeniable challenges for the jurist. The latter, in search of rationalization and clarification, is confronted with techniques and concepts that are often obscure to a person who is not an expert in the field of information technology".
[831] V. Appendix 3 & 6, Focus 1.

diplomas[832] , industrial designs, certificates or KBIS extracts[833]). The latter, for example, involves intellectual property professionals, who will have to rework copyright, trademark and patent technology in the light of blockchain technology. In the end, not all legal professionals will be directly impacted by the various uses of blockchain technologies, but they will certainly be affected by their clients, who will probably be using public, private or hybrid blockchains. It is therefore not a question of considering a total recentralization of decentralized services by trusted third parties such as notaries, lawyers, commissaires de justice[834] , court clerks or chartered accountants, but rather of not denying their qualities, experience and necessities for society. Indeed, their presence and action will guarantee the security of any technical or legal operation linked to one or more transactions on the blockchain, to the benefit of the stakeholders involved. In this respect, it is worth mentioning several pseudo-decentralized services (a private blockchain) currently offered by the Ordre des Commissaires de Justice, in partnership with IBM, thus setting an industrial example in the legal world[835] . Similarly, the "*MonIdenum*" project[836] is a service offered by the Conseil National des Greffiers des tribunaux de Commerce and Infogreffe, enabling company directors to connect quickly and securely to Infogreffe's partner sites (federated digital identity system). The system also uses a private blockchain to enhance the security of information exchanged between registrars and speed up the updating of trade and company registers (RCS), while preventing document fraud, the creation of fictitious companies or the impersonation of company directors.

2.7.1 The role of lawyers strengthened by decentralized identity

In general terms, the decentralized digital identity (IND)[837] will enable lawyers to certify the civil identity of parties involved in a commercial transaction more reliably and transparently. This not only reduces the risk of fraud, but also enhances trust between stakeholders. Where appropriate, lawyers can also use blockchain to securely store certain legal information relating to a transaction, reducing the risk of document forgery and making it easier to verify the authenticity of contracts.

---

[832] BC Diploma and Université de Lille, "Attestations numériques blockchain de réussite au diplôme de l'Université de Lille", Livre Blanc du projet "Dem-Attest-ULille", February 2023, available at.

[833] In reference to a project carried out by Blockchain Partner, in 2018, with the State of Geneva concerning the issuance of *KBIS* extracts thanks to the anchoring of unforgeable and sustainable *metadata* (digital footprints). More information at

[834] Decree no. 2021-1625 of December 10, 2021 on the powers of judicial commissioners, available at the following address, *see* also Chambre nationale des commissaires de justice (CNCJ), available at the following address

[835] In particular, for online statements of facts by judicial commissioners, or to time-stamp data or documents in a similar way to the Soleau envelope, visit www.legide.paris.

[836] For more information, visit monidenum.fr

[837] See *below*, II, Title I, Chap. 1

For the time being, IND remains a niche market compared to crypto-assets, even though these two technological bricks are conceptually grouped together under Web 3.0 in the sense of this study. The IND's impact on the legal professions is therefore as yet little known and anecdotal, but it is suggested that as its adoption progresses, the legal professions will be impacted, particularly in terms of articulating these new IT standards with the rules of law and, by extension, with the progressively digitized lives of lawyers. To reinforce the comments made in the previous section, it is possible to identify and group into four major legal professions the areas that will be impacted by the IND over the coming decade: (i) lawyers[838] , (ii) notaries, (iii) judicial institutions and (iv) judicial commissioners. Firstly, trusted third parties and representatives of the judicial system may use decentralized digital identity attributes (DID, VC)[839] to issue or endorse deeds[840] . Updates to these deeds could be tracked in real time and traced if necessary, using one or more dedicated blockchains (private or consortia to guarantee legal compliance). These possibilities would enable a more transparent and efficient organization of interactions between players in the legal system, thus reinforcing the digital trust of litigants. By way of illustration, blockchain technology is already beginning to be used in their (crypto)activities[841] by some lawyers and in some jurisdictions. In 2022, for example, a hacker received a temporary restraining order ("TRO")[842] from a law firm. This order was sent directly to him in the form of an NFT[843] on his crypto-asset portfolio, allowing a posteriori the freezing of these fraudulent funds under another order from a Liechtenstein court[844] . This situation could mark a turning point for legislators, who could become aware of the technical added value of direct registration and transmission of legal acts or procedural evidence via a blockchain. Far from the a priori view of crypto-assets as facilitators of illicit activities, they can also be an effective means of identifying criminals and protecting Internet users or victims. Closed blockchains represent a high-potential Web 3.0 segment for lawyers, albeit a less sensational one in terms of IT innovation. However, these use cases generate significant needs in terms of rather conventional contractualization, with only the commercial approach appearing to be innovative. For example, the traceability of goods in the transport sector (medicines, food) implies a major need for contractualization. However, unlike crypto-assets, which are currently raising legal issues

[838] SUN Mengqi, "Crypto Industry Can't Hire Enough Lawyers", 2022, in *The Wall Street Journal*, Accessed April 28, 2022, at.
[839] V*, infra*, II, Title 1, 1.3.1
[840] In concrete terms, these actors could acknowledge receipt of a legal act, modify it and send it back in a cryptographically secure way that could be verified by other parties.
[841] See also the Mexican court ruling in the next section.
[842] District of Columbia Courts, definition available online at, "A temporary restraining order (TRO) is part of a civil trial and lasts approximately 14 days. A judge can order a party to do or not do something for this short period, including staying away from and/or having no contact with you."
[843] See *above*, I, Title 1, 2.3.1.1.f
[844] LCX, "Law firm serves anonymous hacker a restraining order via NFT. BTC PEERS". Retrieved June 23, 2022, from, "The 'NFT Service' link leads to legal documents, including the TRO order, at https://www.hklaw.com/en/general-pages/lcx-ag-v-doe".

complex, notably by penetrating new sectors with new functionalities, closed blockchains give rise to few if any new legal issues. Conversely, in sectors such as video games[845] or even corporate law, the introduction of crypto-assets (public blockchains) regularly leads to a new legal approach, as it involves the tokenization of assets, i.e. the use of blockchain technology to transpose the intrinsic characteristics of tangible assets (real estate, movable property) or intangible assets (company shares, characteristics of a character in a video game) to unique virtual representations. This extension and/or duplication from the physical to the digital universe theoretically enables each individual to transfer, immobilize or divide these unique virtual representations. In this research context, and with the now declared desire for tokenization, digital identity could also be subject to an attempt at tokenization, i.e. a form of traceability or financial valuation of certain identity attributes[846] . In terms of data protection under the RGPD, it is important to remember that the latter is neutral towards the technologies used and does not seek to limit any particular technology, but rather to make the person who administers it, i.e. the data controller, accountable. It is recalled that the GDPR does not apply to the whole of the Internet, but only to those in charge of processing data from their applications, and similarly, it does not directly target blockchain technology, but rather its holders and operators. As a result, decentralized digital identity[847] can help

"Data Protection Officer - DPO" to fulfill their mission by reinforcing the security of personal data. Indeed, decentralized digital identity enables identifying information to be securely aggregated and shared only with authorized stakeholders. DPOs will also be able to use a closed blockchain to store evidence of personal data processing activities, which can facilitate compliance audits.

2.7.2 Alternative and decentralized justice with the Kleros protocol

The rise of digital transactions on various public blockchains has inevitably led to an increase in disputes between users, as a result of fraud, theft and loss of crypto-assets. For this reason, new alternative and experimental dispute resolution platforms have emerged on some open blockchains, such as the "*Kleros*" system in 2018[848] or

[845] See *infra*, II, Title 2, 1.4.
[846] To back up these comments, Pascal Gauthier, CEO of Ledger (a company specializing in physical and software security for crypto-assets), explains: "Is tokenized identity your next market? Yes, the combination of money and identity is the future of the physical wallet, the hardware wallet in crypto jargon. We want to provide a solution that will be a kind of everyday companion for users"; "Our ambition goes far beyond crypto", TELLIER Louis, 2022, in *AGEFI*, consulted on October 17, 2022, at the following address
[847] *See below,* II, Title I, Chap. 1
[848] For further information, visit the project website at the following address

"Aragon Network Jurisdiction[849] in 2020. This section examines the Kleros solution, also the subject of Appendix 8, which is specifically dedicated to it, in order to determine whether a public blockchain represents a viable infrastructure for hosting an alternative, experimental and decentralized online justice system. The aim is to understand why adherence to such a proposal is as ambitious and innovative for certain developing countries, as it is uncertain and marginal in the short and medium term in developed countries. On July 31, 2018, the birth of the Kleros protocol proposes a new decentralized application to the digital and judicial sphere[850] . Kleros, a société coopérative d'intérêt collectif (SCIC)[851] , is committed to realizing the promise of a "*decentralized justice system for the internet age*"[852] . Although justice is a regal prerogative, just like the issuance of a legal identity, Kleros seeks to emancipate and democratize this practice through digital means. The Kleros protocol aims to provide a new, effective response to the increase in disputes in the digital sphere due to the growing number of Internet users interacting and consuming online[853] . In 2020, Kleros received an award from the European Innovation Council with funding to the tune of one million euros to develop decentralized digital justice[854] . From a social science perspective, Kleros relies on collective intelligence - on a "*wisdom of a crowd of participants*"[855] - to resolve disputes via a supposedly decentralized and incensurable digital space. With Kleros, every decision taken by a jury of pseudo-anonymous, crypto-asset-holding Internet users reflects the collective wisdom of this crypto-community. These jurors are incentivized to act honestly when adjudicating disputes, as they are economically constrained in the event of decisions contrary to the collective morality. In theory, this alternative system makes it possible to arrive at a form of collective truth. It originates from the social experiment of "*The Wisdom of Crowds*"[856] , and has been transposed by Kleros to Web 3.0. This distributed ecosystem considers that this community wisdom approach does indeed enable morally just, even impartial, judgment[857] . In practice, the modus operandi proposed by Kleros is to make a new dispute resolution protocol available to all Internet users, enabling them to decide

[849] "Aragon Network Jurisdiction Part 1: Decentralized Court", 2021, in *Aragon's Blog,* available at
[850] *Op. cit.* "(...) the blockchain carries in its blocks and chains a veritable theory of justice (...)", "Justice digitale", p. 157.
[851] To find out more about *SCIC Kleros*, visit the following address
[852] Kleros page presentation, p. 2, accessed online April 21, 2021.
[853] With the progressive digitization of our society, digital contracting is booming and, by trickle-down effect, many digital disputes are arising. In this sense, and because the number of online buyers is increasing (via e-commerce), then a proportional increase in digital disputes should continue to grow in the future. Statista, "Digital buyers worldwide 2021", consulted online April 22, 2021.
[854] EC, Shaping Europe's digital future. "The Commission's European Innovation Council awards €5 million to blockchain solutions for social innovations.", June 30, 2020, available at.
[855] SUROWIECKI James, "The Wisdom Of Crowds", 2005, in *Anchor Books*, ISBN: 0-385-72170-6, accessed online November 21, 2021, p. 53.
[856] *Ibid.* These are all attempts to harness the wisdom of the crowd, and that's why they work. It turns out that the real key is not so much to perfect a particular method as to fulfill the conditions - diversity, independence and decentralization - that a group needs to be intelligent." Read pp.119-121 about Professor Thomas C. Schelling's social experiment.
[857] In reference to a series of days and workshops on the subject of Kleros: "Workshop - Decentralized Justice" - EHESS - November 18, 2022 10:30am-5pm, organizers: Katrin Becker (Univ. Luxembourg) et al. Venue: EHESS, 54 boulevard Raspail 75006 Paris - room A06_51.

through intelligent contracts on the Ethereum blockchain[858] - disputes of all kinds, also submitted by Internet users. In concrete terms, the Kleros protocol combines blockchain technology with online community collaboration ("*crowdsourcing*"[859]), to resolve claims and disputes online. This innovative coordination characterizes a form of attempted online judicialization, which touts its openness and transparency in the service of a fairer, more open Internet. This project is thus in line with a certain desire and idea to reinvent social justice, from the rule of law and its institutions, towards justice for Internet users and by Internet users. To function, this decentralized architecture relies on economic incentives to motivate pseudo-anonymous Internet users - the aforementioned *jurors* - to rule as closely as possible to the truth on the basis of each dispute submitted directly to the website and platform maintained by Kleros[860] . The system is based on a number of theoretically random selection principles for these citizen-jurors, a universe borrowed from the Athenians and Ancient Greece both conceptually and democratically, as well as mercatically[861] . In this context, the use of blockchain technology and crypto-assets offers a solution to a problem already raised by Aristotle several centuries ago: "*he who controls the courts, controls the state*"[862] . In other words, legal transparency is essential to any judicial system, and litigants must be able to have confidence in the integrity of the judicial process, including the selection of judges and the authenticity of the evidence presented. To meet this challenge, Kleros uses *game-theoretic* incentives[863] and crowdsourcing to help jurors judge cases fairly and impartially. The Ethereum public blockchain verifiably and permanently records all online dispute resolution processes submitted to Kleros. Would this public blockchain therefore enable us to optimally meet the transparency requirements of a new 3.0 justice system?[864] . At this stage, it seems that this is only partly the case. Indeed, as compromises at the expense of other social and legal components arise, it is indeed pertinent to look at four fundamental questions and challenges that Kleros must address[865] : is the system truly computationally decentralized? How can we trust

---

[858] V. Appendix 6, Focus 2.

[859] *Crowdsourcing* consists in drawing on the knowledge of a community and a crowd of Internet users to achieve a given social result.

[860] See the Kleros platform at the following address, *see* also Appendix 8.

[861] In Greek, "Kleros" means "luck". In ancient Greece, a "cleruchy" ("klêroukhía" in ancient Greek) was the allocation of plots of civic land ("kleros") to soldier-citizens by lot. These soldier-citizens were called "clerics" (who were present in Athens in the 5th and 4th centuries BC). The term "kleros" therefore referred to the plot of land allocated to a citizen by lot. C. Vial, *Lexique de la Grèce ancienne*, A. Colin, 2008.

[862] MIRHADY David C., "Aristotle and the Law Courts", Polis J. Anc. Greek Polit. Thought, 2006, accessed April 22, 2021.

[863] To understand this concept in computer science, we can refer to the following explanation: "Satoshi Nakamoto taught us that a number of anonymous computers that do not trust each other can nevertheless reach a consensus, provided that economic incentive mechanisms are properly structured. Kleros extends this principle to human decision-making. A number of anonymous jurors who don't trust each other can still *reach* a consensus on a good decision, provided the incentives are properly structured", AST Federico, "Kleros
: Frequently Asked Questions about Peer-to-Peer Justice", 2017, in *Medium*, available at.

[864] The term *3.0* refers to a comparison between *LegalTech*, which offers centralized digital services *(2.0)*, and blockchain technology, which offers decentralized online services *(3.0)*. So, because the degree of informatics required for blockchain seems greater than for *LegalTech 2.0*, the term *3.0* becomes relevant as well as technologically distinctive.

[865] V. Appendix 8.

in this pseudo-institution that substitutes for the courts, given omnipresent technological uncertainty? In the end, is Kleros really doing justice in the sense of the law, or rather in the sense of its community of Internet users?

The platform requires users to hold and use a[866] digital utility token.
"*PNK*"[867] . It is emphasized that Kleros users are not required to master computer programming to use the smart contracts developed by the platform, as these are designed to be relatively easily accessible via its platform. The use cases and disputes targeted by this innovative service are, in theory, numerous[868] , but for the time being seem rather marginal and confined to the world of crypto-assets and, at most, certain other Web 3.0 domains (Metavers[869] , NFT). Kleros has found a solid base in the world of crypto-assets, where it can optimally deploy its functionalities by creating a philosophical conception of justice that differs from the conventional legal system. Decentralized Finance (DeFi) is also an ecosystem composed of multiple pseudo-decentralized protocols, where regularly aggrieved users can now turn to Kleros to obtain a form of justice in the event of loss or extortion of their crypto-assets, or to challenge misleading information provided by crypto-asset exchange platforms[870] . Nevertheless, the bankruptcy of the "FTX" platform and crypto-exchange[871] , which hit the headlines in 2022, has led to an increase in demand for decentralized protocols, consequently benefiting Kleros. From a computational science perspective, Kleros addresses the so-called "*Sybil*" problem[872] , which involves preventing the duplication of false identities by jurors, who could thus manipulate the collective decisions of this online crypto-community. There are many public blockchain mechanisms that more or less perfectly solve the Sybil attack problem, thanks in particular to (crypto)economic incentive mechanisms[873] of unequal effectiveness, such as Proof of Work ("PoW"), Proof of Stake ("PoS") or Proof of Authority ("PoA"), which are examined in Appendix 6. Kleros should be described in terms of its potential and limitations. The methods

---

[866] As we explained in the section dedicated to crypto-assets, the *PNK* is a *utility token* and its economic incentive aims to encourage its use on the Kleros protocol and applications.
[867] Several thousand years ago in ancient Greece, a *pinakion* was a small bronze plate used to identify the citizen of a city by displaying his or her name. It was a form of *citizen token*. Candidates for political office or jury duty would insert their *pinakion* into a machine called a *klerotèrion*, to be drawn by hand. The Kleros project thus takes its name and its digital token (PNK) from this emblematic tool and era of ancient Greece, sometimes considered the cradle of democracy.
[868] Online gaming, intellectual property disputes, healthcare, social media, participatory financing, self-employed workers, etc.
[869] See *infra*, II, Title 2, 1.4.
[870] Kleros allows any user to submit a dispute, which means that if a decentralized protocol or centralized exchange platform provides incomplete or erroneous information to its users, the latter can take action against them via Kleros. This is also possible in the case of "*proof of reserve*".
- *PoR*") of these entities, which may be more or less accurate and yet essential for creating and ensuring the trust of crypto-users.
[871] Contributors to Wikimedia projects, "FTX bankruptcy", 2023, available online
[872] V. Appendix 6, Focus 1.
[873] V. Appendix 6, Focus 1 to 3.

Alternative Dispute Resolution (ADR)[874] is an example of the decentralization that Kléros is interested in, whether the disputes are judicial (court-ordered) or conventional[875] , i.e. agreed between the parties to a dispute. As the Kleros protocol and its underlying Ethereum blockchain[876] evolve, it seems that this decentralized justice system may one day be able to resolve increasingly complex disputes. An update of Kleros is scheduled for deployment in 2023. For the time being, Kleros is already enabling the widespread use of smart contracts in a small but growing number of crypto-economic activities. However, the Kleros proposal does have certain limitations that are worth mentioning. For example, its (crypto)fees, i.e. the cost of using it, are quite significant: as the number of users of the Ethereum blockchain increases, the fees paid by Kleros users mechanically increase[877] resulting in an increase in the price to be paid to become a juror on Kleros[878] . This is a difficult economic consequence for lawyers, who believe that justice should be accessible and free[879] . Kleros is already attempting to deploy certain solutions to deal with these problems of volume and limited scaling of the blockchain on which it operates[880] . The economic incentive provided by the PNK also hinders Kleros' operations, as the majority of tokens are centralized in a few individuals and companies[881] . In 2023, the Kleros solution will operate on a small scale for a few hundred or thousand individuals, but will remain inaccessible to a larger number of Internet users. Despite its effectiveness in many cases, it must be recognized that Kleros has a major limitation: it remains a mathematically binary system, and therefore not very adaptable to the complexity of disputes requiring professional knowledge of law and procedure. These skills can only be provided by lawyers from regulated professions, which limits the scope of Kleros in certain situations. It appears that

---

[874] ROLLAND Paul, doctoral student, "Les Modes Alternatifs de Règlement des Différends (MARD)", in *Village de la Justice*, accessed April 23, 2021, *see* also the provisions of articles 131-1 to 131-15 of the Code of Civil Procedure governing court-ordered (so-called judicial) mediation and those of articles 1530 et seq. of the same code for so-called conventional mediation.

[875] Conseil d'Etat, Étude annuelle 2014, Le numérique et les droits fondamentaux, accessed November 20, 2021, see also Conseil d'Etat recommendation no. 3: develop mediation to settle disputes related to the use of digital technologies.

[876] V. Appendix 6, Focus 2.

[877] To become a juror in a Kleros Court, a minimum of *1000 PNK* must be held in escrow.

[878] The variation of transaction fees on a blockchain is automatic and protocol-based. The law of supply (computers validating transactions) and demand (users wishing to carry out transactions) applies. So, the more users demand transactions, the more the computers that validate the transactions become - temporarily - unable to meet this demand, which mechanically increases transaction costs. V. Appendix 3, Focus 1 to 4 and Appendix 6, Focus 1.

[879] Justice is a common good that may have a cost, but should not have a price: in the traditional judicial system a judge is paid to render a verdict by virtue of his skills and power, so for Kleros to charge jurors to render justice is in fundamental opposition to our current judicial functioning.

[880] The Ethereum blockchain underwent a major protocol update in 2022 ("The Merge" also known as "ETH 2.0"), which can ultimately reduce transaction costs. For example, the XDAI solution and Polygon, which enable transactions to be carried out at lower cost, although these solutions are IT-centralized (IT recentralization), see *above*, I, Heading 1, 2.3.2.

[881] In this respect, Vitalik Buterin believes that "To trust a service such as Kleros, it seems necessary that no single individual should hold more than 25% of the tokens in one of these digital courts", "DAOs are not corporations: where decentralization in autonomous organizations matters", 2022*, op. cit.* available at the following address

that Kleros currently lacks a political space for speech, like a traditional justice system. This means that the platform is not yet able to recreate some of the essential human elements of the physical world. Although the Kleros solution enables partially reliable direct democracy through its community voting, it remains an alternative that does not allow for the expression of speech in the form of real-time video, voice messages and so on. Consequently, it seems that Kleros needs to implement a political space where the word of its jurors or the parties to a dispute can be expressed - through testimonies, conclusions, pleadings - in order to ensure more humanity and less determinism through calculation (implied by FACs). Lawyers studying Kleros note the use of a mercantile vocabulary similar to that of the law, although Kleros is in no way a judicial tribunal, even if it aims to reproduce the effects of one[882] . According to Aurélie Jean, justice and the exercise of the law are first and foremost a matter for human beings, for the individuals who are being judged, whether as plaintiffs, victims or defendants[883] . What's more, judges must take into account what the collective considers to be fair in a given dispute, based on the evidence presented by the jurors, who lose their sequestered funds when their decision is in the minority in a dedicated vote. So there is no common law to enforce, but rather a collective morality that judges each dispute on a case-by-case basis. In reality, this collective morality is based on the mentalization (conscious or otherwise) of each juror's own laws, as jurors in practice base their verdict on the law in force. It should also be noted that only contractual disputes for which an arbitration clause has been provided for could benefit from recognition and legal value when resolved by the Kleros protocol. On the other hand, other disputes which have not been contractualized beforehand have no legal basis other than moral, except for the exchange of PNK tokens between the parties, which could be considered as a form of tacit contractualization. In accordance with the New York Convention, for example, it is noted that the Kleros platform cannot be considered a legally valid form of arbitration[884] . In this respect, four elements are identified that make Kleros at odds with the current judicial system: (i) its decentralization, (ii) the immutability of the transactions carried out, (iii) the quasi-anonymity of the jurors and (iv) the binarity of its computer code mentioned above. In practice, the decentralized nature of Kleros is relative, since intermediaries and operators are easily identifiable on social networks, an observation that the European legislator will probably enforce if Kleros does not register as a PSCA in accordance with the entry into force of the MiCA Regulation, as well as TFR as a "financial intermediary".

---

[882] LEQUESNE-ROTH Caroline, "Metavers, Web3 : la révolution juridique en trompe-l'œil", in *Receuil Dalloz,* 2022, "The legal community is expected to take part in the legal battles that will be waged, and more broadly in the legal arbitrations that will crystallize civilizational choices. If the announced legal revolution is a trompe-l'œil, the inclusion of digital law in our democratic values and respect for our fundamental rights is one of the major challenges facing the lawyer of the 21st century", available online, p.5.

[883] JEAN Aurélie, "Les algorithmes font-ils la loi?", *op. cit.* reading position in the book: 82%.

[884] FERREIRA L.C., "La résolution des litiges blockchain : Vers un arbitrage décentralisé ?", Master's thesis, University of Neuchâtel, 2021, p. 96, "Even if, depending on the circumstances of the case, a Kleros decision could theoretically be qualified as a foreign arbitral award within the meaning of art. I ch. 1 CNY, the procedure suffers from a number of anomalies which prevent such a characterization"; "When the Kleros procedure is delocalized, in the sense that it is not linked to a legal order, the New York Convention does not apply".

previously discussed. Similarly, the immutable nature of transactions and certain information relating to disputes (documents and supporting evidence) that are published in non-compliance on the Kleros platform disregards the principles of the RGPD for the time being[885] . With regard to the territoriality of applicable law concerning disputes managed by Kleros, its decentralized and borderless nature, coupled with the pseudo-anonymity of its users' transactions, complicates the actual location of the dispute[886] . In procedural terms, the creation of alternative procedures on Kleros does not respect certain provisions imposed by international arbitration rules (physical testimony of the parties[887] , right to a fair trial)[888] . So, while the theatricality of proceedings is sometimes criticized or even mocked (gowns, legal jargon), it is in fact essential to guarantee the neutrality of the roles, fairness and impartiality of legal decisions. The widespread adoption of Kleros would run the risk of gradually erasing the humanity of legal proceedings, such as pleadings and the humanism of jurists. To remedy this, it seems that the Kleros protocol could integrate its own Metaverse[889] in the future, enabling deliberations to be organized with avatars (jurors could decide to remain pseudo-anonymous). The use of Ricardian Contracts, already mentioned, would also appear to be relevant to the Kleros protocol, in particular to optimize the articulation between smart contracts and any associated natural language contracts. In a way, Kleros applies the principles of gambling and speculation to the legal system, enabling users to earn money in the form of crypto-assets while currently rendering pseudo-judgments with regard to Western legal systems. However, to ensure the long-term viability of this system, it is essential that its community operation and economic incentive mechanisms are transparent and fairly distributed among users[890] . It is likely that, in a conflict between the Kleros system and the traditional legal system, the law will consider the user-juror as a simple investor with no legal jurisdiction due to his pseudo-anonymity. This pseudo-anonymity could be a weakness in the event of a technical or democratic failure of the Kleros protocol, and the implementation of identification through decentralized digital identity (IND) standards would seem relevant (implementing a form of pseudo

[885] In 2023, it is possible to find the personal data of "justiciables" on the Kleros platform with just a few clicks, as the documents are accessible to any Internet user. Thus, RGPD compliance is not currently assured by this 3.0 service.
[886] The KLEROS protocol does not take into account the differences in territoriality and legal culture of judges who do not know each other due to their respective pseudo-anonymity.
[887] *Ibid*: "[...] written or oral language was an essential step in the work of elaborating the truth. The purpose of written transcription or oral testimony was to articulate a legal text to an extra-legal reality", p. 175.
[888] "[...] alongside logical reasoning on the part of the representative of the law came a certain emotional intelligence to consider the litigant as a unique being with a history and a past that belong to him and that are, by definition, unique and irreproducible.", *op. cit*., JEAN Aurélie, "Les algorithmes font-ils la loi?", reading position in the book: 81%.
[889] See infra, II, Title 2, 1.4.
[890] As of November 11, 2022, only ten Ethereum addresses (out of more than 9,000) hold more than 50% of the total PNKs in circulation, meaning that PNK token distribution is relatively centralized to date. "*Pinakion Token Contract and Distribution Chart*", information available and verifiable at the following address

hybrid anonymity)[891] . However, it should be stressed that the current justice system is not perfect[892] either, and that the technologies and concepts used in Kleros, such as DAO and AEC, could be useful if they involve legal professionals. Kleros offers a new definition of online justice, but this redefinition must not be to the detriment of the notions of integrity and honor that underpin the current legal system, yet are absent from Kleros for the time being.

In short, Kleros is an innovative concept with the advantage of offering an imperfect alternative to the traditional system, such as Alternative Dispute Resolution (ADR) via this protocol. This experimental, decentralized trusted third party enables its community to resolve certain financial disputes relating to the use of smart contracts already in use in the crypto-asset ecosystem, particularly in the field of Decentralized Finance. Although Kleros is partly in opposition to the traditional judicial system and dependent on its recognition in developed countries, it is important to consider this project as a fair and relevant alternative in countries where justice is weakened. In practice, Kleros has already become the preferred decentralized justice system for resolving disputes within the crypto-economy, as evidenced by an initial court ruling in Mexico[893] . The solution proposed by Kleros is also relevant, as it leads us to question the current structure of our own judicial system. In other words, Kleros represents a symptom of the current malaise regarding certain limitations of our justice system, which suffers, among other things, from a lack of human resources and digital outlets. It will be up to jurists to embrace or reject these experimental systems of alternative justice 3.0, but it already seems important to explore and deepen possible synergies with this maturing system. As the Swiss jurist Léonel Constantino Ferreira rightly suggests, "*from a co-regulatory perspective, the state could limit itself to setting a general procedural framework for blockchain dispute resolution, while leaving it to the technology's participants to develop precise standards and mechanisms for implementing them*"[894] . However, Kleros does not operate in a non-existent legal framework, which means that it needs legal recognition in the long term if it is to survive. It needs to implement a hybrid solution so that its form of moral and collective jurisprudence becomes compliant with current laws and regulations (RGPD, MiCA, TFR, eIDAS, Data Act). According to an EHESS working group dedicated to this phenomenon of decentralized justice, this system of quasi-justice is already viable for dispensing justice in certain developing countries where states are not rule of law due to a

[891] *Jurors* could remain pseudo-anonymous, while designating *juror-referents* (with a law degree) as support if necessary.
[892] Unfortunately, we are rediscovering that without a society united around the values that underpin a right, its fundamental and universal dimension can be called into question, in a single day, by a handful of people (constitutionalists, parliamentarians), while this decision will impact millions.
[893] Kleros, "How to enforce Blockchain dispute resolution in court? The Kleros Case in Mexico", 2022, available at, "Thus, for the first time, a Mexican court recognized and enforced an arbitral award whose substance was not governed by the arbitrator's judgment alone, but by a technological tool designed for decentralized dispute resolution: the Kleros protocol."
[894] *Op. cit.* FERREIRA L.C., "La résolution des litiges blockchain: Vers un arbitrage décentralisé?", p.95.

corruption of the judiciary[895] . This decentralized justice system could be considered more reliable in certain Latin American or Indian countries, where many Kleros users are already located. It is also likely that the growth and success of Kleros will depend on the overall growth of Web 3.0, which includes multiple technologies in phase (crypto-assets, virtual reality, Metavers, IND). It seems that to succeed in achieving their openly stated theoretical ambition - "*Decentralized Justice as a Service*" - Kleros will need to attract other physical and virtual communities, particularly lawyers, to provide structural support for its deployment. As far as digital identity is concerned, while the Kleros protocol has successfully proposed a decentralized justice system with a relatively low degree of identification (level 1 or 2)[896] , there can be little doubt that the implementation of a self-sovereign digital identity (INAS) specific to the Kleros protocol, seems imminent. Thanks to this digital identity on a blockchain, Kleros could become a decentralized identity provider not only for its own decentralized justice service, but also for third parties and online services (PSCA) seeking verifiable identifiers and digital identities. Eventually, the line between decentralized justice and self-sovereign digital identity could blur to the benefit of Kleros users. Perhaps, one day, this decentralized online justice will even feed into certain components of predictive justice (using artificial intelligence).

2.8 Blockchain technology as a tool for legal proof

As blockchain technology gains adoption within society, more and more legal professionals are faced with a new question relating to law and IT 3.0

Is blockchain technology an unrivalled new evidential tool? Some proponents of this technology often describe it as a preferred tool for reliable dematerialized evidence, due to its accessibility, supposed affordability, programmability and relative immutability. Consequently, it is important to ask how French evidence law frames and recognizes this technology perceived as the ultimate source of digital evidence. First, it is worth recalling the two guiding principles of French evidence law, within which blockchain technology must fit in order to be considered an admissible means of proof. Indeed, the French civil and evidentiary system is based on the principle of legal proof, which is legally organized and framed, as opposed to moral proof, which admits all possible means of proof. The system of legal proof in French law is based on a number of essential legal aspects, including five different categories of evidence, as follows

[895] In a corrupt country, decentralized justice is probably better than a corrupt judicial system. It represents a counterweight to censorship.
[896] See dedicated diagram, *v, supra*, I, Title 2, 1.4.1

by the Civil Code[897] : (i) literal or written evidence, (ii) testimonial or testimonial evidence, (iii) judicial presumptions, (iv) judicial admissions and (v) decisive oaths. As such, each has varying admissibility and probative value[898] . In principle, the system of legal evidence governing legal acts requires them to be proven by written documents, which are considered to be perfect proof and irrebuttable. Legal facts, on the other hand, are governed by the system of moral evidence, and can be proven by any means, i.e. by what is known as imperfect evidence. The probative value of the five aforementioned modes of proof is not equal. Certain types of evidence, such as written proof (i), judicial confession (iv) and the decisive oath (v), are considered perfect and probative, and are binding on the judge without any possibility of questioning their existence or basis. On the other hand, other types of evidence, such as testimony (ii) and judicial presumptions (iii), are imperfect and leave the power of conviction to the judge's sovereign discretion. Consequently, short of amending the Civil Code to create a sixth category of evidence specific to the probative nature of blockchain technology, it would seem preferable initially to attach the information contained in a blockchain to one of these five categories of legal evidence. Although, in principle, the probatory value and admissibility of the various modes of proof listed are fixed by law, not all of them are admissible as proof of all elements relating to legal acts or facts. In this respect, article 1358 of the French Civil Code requires a two-stage analysis. The latter states that proof is free: "(...) *proof may be provided by any means*", suggesting that all modes of proof are freely admissible. However, it goes on to specify that "*in cases where the law provides otherwise* (...)" free proof is subject to certain exceptions cited by the Civil Code. One of these legal exceptions concerns the proof of legal acts with a value in excess of €1,500, which must necessarily be administered by means of literal proof, i.e. by a written document[899] whose probative value is perfect as mentioned (as long as its integrity can be traced and established). Depending on the mode of proof used, the effect on the judge may vary in cases where proof is free. It is therefore essential to classify blockchain technology in one of the existing categories of French evidence law in order to determine the probative value of digital evidence on a blockchain. If 'blockchain evidence' is considered perfect evidence, the judge will be obliged to take it into account. However, if it is considered imperfect evidence, the judge could decide not to take it into account depending on the circumstances[900] . It should be pointed out that French law was a forerunner in admitting evidence

[897] Art.1363 to 1386-1 of the Civil Code, amended by Ordinance n°2016-131 of February 10, 2016.
[898] Art. 9 of the Code of Civil Procedure: "It is incumbent on each party to prove, in accordance with the law, the facts necessary for the success of its claim".
[899] This writing must be an authentic deed (art. 1369 of the Code of Civil Procedure), a deed under private signature (art. 1372 of the Civil Code) or a private deed countersigned by a lawyer (*see* the Deed of Lawyer).
[900] A judge (or forensic expert) needs to understand the governance of a blockchain in order to interpret the probative value of a data entry within it. This same governance, which is specific to each blockchain category, is capable of affecting the integrity of an entry, modifying its content and its existence.

[901] for over twenty years[902] . This legislative and technological advance has made it possible to grant equivalent probative force between evidence on a material medium (handwritten signature) and evidence on a dematerialized medium (digital signature). In this respect, the dematerialization also possible thanks to blockchain does not represent a limit in terms of admissibility as a mode of proof, in accordance with article 1316-1 of the law of March 13, 2000 on the adaptation of the law of evidence to information technologies. However, the recognition of electronic evidence is subject to certain irreducible specificities[903] , which may influence the strength and conviction of electronic and intangible evidence compared to tangible and material evidence. Because evidence of information recorded on a blockchain is electronic, it must in principle be admissible by any jurisdiction, but this legal admissibility must not be confused with the assurance of legal recognition. For an electronic document to be able to produce its legal effects effectively, the judge must necessarily be convinced of the integrity of the computer system used, and therefore first understand the mechanisms and workings[904] . Because these debates on the substance and form of electronic evidence on blockchain are complex, the eIDAS regulation stipulates that a presumption of validity of said evidence exists, provided that the time-stamping in electronic form meets the requirements of a qualified electronic time-stamping[905] .

In addition to the foregoing, it would seem legitimate to dwell on the role of the notary, who is a ministerial officer essential to the production of perfect evidence through the authentic instruments he issues. The probative force of a notarial deed only concerns deeds that the notary has personally performed or witnessed. In practice, the notary is a trusted third party of the State, governing relations between the State and taxpayers. Notarized deeds have a probative value that cannot be challenged by a judge, and only apply to deeds that the notary has personally performed or recorded. As trusted third parties of the state, notaries govern relations between the state and its citizens, forming a kind of 'human and institutional infrastructure' by virtue of their regulated role. However, unlike a blockchain infrastructure, notaries guarantee the social and legal balance of agreements between parties, conferring a superior probative value on the associated deeds. Even in comparison with imperfect proof based on blockchain and associated with a convention on proof, an authentic notarial deed remains the most

---

[901] Pursuant to art. 46 of the European eIDAS Regulation, "The legal effect and admissibility of an electronic document as evidence in legal proceedings may not be denied on the sole ground that the document is in electronic form".
[902] Law no. 2000-230 of March 13, 2000 adapting the law of evidence to information technologies and relating to electronic signatures, *v.* Ordinance no. 2016-131 of February 10, 2016 reforming the law of contracts, the general regime and the proof of obligations.
[903] Art. 1366 of the French Civil Code states that "An electronic document has the same probative value as a paper document, provided that the person from whom it originates can be duly identified, and that it is drawn up and stored in conditions that guarantee its integrity".
[904] Thanks to a legal expert or commissioner who submits a detailed and simplified technical report to the judge where necessary.
[905] See *infra*, II, Title 1, 2.1.1.1.

reliable, as it can only be challenged in the event of a forgery, whereas an agreement on proof has only a simple presumption of reliability, which can be challenged. The conditions and scope of this type of agreement remain limited[906] . For example, when a jurist whose profession is regulated (notary, commissaire de justice, lawyer) is involved[907] , a digital evidence agreement may appear excessive and disproportionate to the authentic force of a deed issued by a notary. Nevertheless, the origin of disputes involving transactions and evidence on blockchain today mainly concerns events that often do not involve notaries, but for the time being rather lawyers. As a result, the use of evidence conventions for these common, private-signature acts seems a temporary solution that users of public blockchains may prefer, until some legislators eventually recognize the presumption of reliability of certain public blockchains.

As a result, the notary will continue to have a monopoly on perfect proof, an "evidential grail"[908] that blockchain technology cannot achieve due to its binary and inflexible nature. For some technophiles, however, public blockchains such as Bitcoin and Ethereum represent sources of digital truths deemed inalienable and therefore close to this "evidential grail", in its acceptance in reality mainly computer-based. From this perspective, blockchain is not intended to replace the key roles of notaries, but rather to provide a new IT infrastructure that notaries can use to certify certain deeds more efficiently. To give probative value to information available on a blockchain, a legal fact can be coupled with a digital evidence agreement[909] , provided that this mode of registration on blockchain is the one retained in this agreement. However, this legal framework is rather paradoxical: if blockchain technology still requires an agreement on proof, this suggests that it does not intrinsically, i.e. cryptographically, have probative value with regard to these texts. Since June 16, 2020[910] , the Notaires du Grand Paris (the Presidents of the 5 Chambres des Notaires franciliennes) have signed a "Politique de Confiance de la Blockchain Notariale - BCN" and set up the Autorité de Confiance numérique notariale des Notaires du Grand Paris to enable the provision of notarial services based on closed blockchain technology. A private blockchain

[906] Art. 4 of Order no. 2016-131 of February 10, 2016: "1°Art. 1356. - Contracts on evidence are valid when they relate to rights of which the parties have free disposal. 2° Nevertheless, they may not contradict irrebuttable presumptions established by law, nor modify the faith attached to confession or oath. Nor can they establish an irrebuttable presumption in favour of one of the parties", see also art. 6 of the Civil Code: "No special agreement may derogate from laws concerning public order and morality".
[907] L'HERMITE Marie and STENNE Paul, "La preuve, la blockchain et les professions réglementées", *Op. cit.* p. 8, "Thus the AMF considered that the intervention of a third party such as a lawyer, bailiff or notary could constitute a guarantee of reliability, operability and effectiveness to ensure the monitoring and safeguarding of funds from ICOs."
[908] Cour de cassation, Colloques sur la blockchain et la Preuve, February 27, 2020, Augustin AYNES (moderator), Bertrand BONNEAU (speaker), Didier FORNONI (speaker) et al.
[909] Art. 1356 of the Civil Code: "Contracts concerning proof are valid when they concern rights which are freely available to the parties. Nevertheless, they may not contradict irrebuttable presumptions established by law, nor modify the faith attached to confession or oath. Nor can they establish an irrebuttable presumption in favor of one of the parties". [910] Notaire du Grand Paris, "Présentation de la Blockchain Notariale (BCN)", Press kit of July 7, 2020, accessed on 27/04/2021.

has been integrated into the IntraNotaires platform[911] to enable the profession to familiarize itself with this technology and its various concrete uses for the profession[912] . At the same time, there are other hybrid initiatives by judicial commissioners, such as the solution developed by the company Smart Preuve[913] , which enables attestations to be generated and then time-stamped, or online statements of facts[914] produced by judicial commissioners using an intuitive mobile application linked to a closed blockchain. However, online statements of facts (with or without a blockchain) may suffer from certain shortcomings in terms of recognition and legal value. A court commissioner will not use a digital application such as Smart Preuve to verify the content of an online photo, but only its receipt and existence. Indeed, for a statement of facts drawn up by a judicial commissioner to be valid, the latter must be physically present at the time of the statement of facts[915] . Although this solution developed by SmartPreuve is not a Holy Grail of proof, it does help to make the law accessible and intuitive for the general public, while representing a sometimes beneficial alternative for pre-litigation and certain everyday disputes. For the time being, it seems that information recorded in a public blockchain is considered natively as imperfect evidence, i.e. whose probatory value can be simply called into question by providing evidence to the contrary[916] . This is because, according to the texts in force, such information cannot be considered as a judicial confession or as a decisive oath, which leaves as the only possible means of perfect proof written proof in the form of an authentic deed or a private deed (convention on proof). According to article 1316 of the French Civil Code, written evidence consists of a series of signs or symbols having an intelligible meaning, regardless of their mode of transmission or medium. However, by using the[917] cryptographic hash technique commonly used for certifying

---

[911] For more information, visit this platform at the following address

[912] L'HERMITE Marie, STENNE Paul, "La preuve, la blockchain et les professions réglementées", consulted online on 28/12/2021, p.2., "notaries and bailiffs have chosen to innovate and thus present themselves as an 'augmented' (by blockchain) notary or bailiff".

[913] This solution is the initiative of 70 French Commissaires de Justice. For more information, visit the following address

[914] A distinction must be made here between a constat and an attestation issued by a commissaire de justice, as their respective legal values differ. Unlike an attestation, a statement of facts makes it possible to obtain an official report, i.e. irrefutable and indisputable proof.

[915] LAHER Rudy, "La numérisation des activités de l'huissier de justice", in *Cah. Droit Sci. Technol*, PUP, 2020, consulted online January 15, 2022, "The protection of litigants' rights and the practical imperative of a physical presence justify this state of affairs". It is therefore imperative that an on-site inspection be carried out by a judicial commissioner.

[916] With reference to the irrebuttable nature of perfect proof, the burden of which cannot be reversed, *see* Art.1354 of the Civil Code : "The presumption that the law attaches to certain acts or facts by holding them to be certain exempts the person in whose favour it exists from having to prove it. It is said to be simple, when the law reserves proof to the contrary; it is said to be irrebuttable when it cannot be overturned".

[917] This cryptographic fingerprint (*hash*) can be derived from a "*Merkle tree*" or "*hash tree*" ("*Merkle Root"),* invented by *Ralph Merkle* in 1979. A *Merkle Root is* a cryptographic tool for consolidating large quantities of data into a single, unique *hash.* This unique *hash* (*Merkle Root*) acts as a cryptographic seal that summarizes a set of captured data. *Merkle trees* enable users to verify whether specific content has been included in a particular set of "*sealed"* data. In the case of Bitcoin, they enable the creation of a unique *hash* containing all the transactions in a block. In the case of a blockchain, the *hashing* process is based on the contents of the block, i.e. the *hash of* the previous block containing a certain number of transactions, enabling each transaction to be automatically time-stamped. The *hash* of a set of data can thus be compared with a precise and unique *digital fingerprint.* A *hash function* is said to be "*one-way*": it is designed in such a way that

documents with blockchain technology, it seems that this method does not meet the notion

"In other words, the dematerialized nature of the technology poses no problem. In other words, the dematerialized nature of the technology poses no problem; the difficulty lies in the ability of a blockchain to meet this intelligibility criterion, even though it may be interpreted by a judge or forensic expert, as previously assumed. As a reminder, in computer science, the purpose of a blockchain is not to store documents directly within it (in its transaction blocks)[918] , but rather to certify them with a unique, inviolable and non-repudiable digital fingerprint. Thus, a digital identifier or

A "hash"[919] embedded in a blockchain transaction cannot be considered as an electronic document, i.e. be given legal value. In legal terms, then, blockchain is not a register of legal evidence, but a tool for cryptographic evidence, imperfect in legal terms without a convention on evidence. Equally, if a blockchain entry is not made in accordance with the conditions required by law[920] , it will not be binding on the judge, as a result of his or her sovereign discretion. In practice, private deeds generally contain the electronic and cryptographic signatures of the parties involved[921] . In the future, it is possible that blocks of transactions containing the electronic signatures of the parties and complying with the formality of the double original and handwritten mention could be considered as acts constituting literal evidence under private signature, provided this is in line with the rules in force[922] . For the time being, therefore, a blockchain inscription can neither constitute a private deed nor an authentic deed, and is therefore imperfect evidence that could be the equivalent of testimony[923] . In fact, this comparison seems relevant in the sense that a blockchain transaction is electronically registered in a block, whose witnesses - in this case, validator nodes - are responsible for validating new blocks, so that each transaction is validated individually and then collectively by these nodes.

---

the fingerprint and *hash* produced are impossible to reverse in order to recover the original information (at least with the computing power available today). Consequently, modifying the content of a block means recalculating the *hashes* of all the blocks that follow it. This characteristic of hash functions means that any modification to the content of a block is immediately visible in subsequent blocks, even if the modification is minimal: this digital imprint constitutes cryptographic - and not legal - proof of integrity for the data initially "*hashed"* by this algorithm. See also Appendix 6, Focus 1.

[918] V. Appendices 3 and 6.

[919] As a reminder, "*checksumming*" or "*hashing*" is a technique that consists in creating a unique fingerprint linked to a piece of information/data. In this way, a piece of data corresponds strictly to a sequence of unique digits and numbers, and a number corresponds strictly to that piece of information (see the following website to transform a piece of data such as one or more words into one or more *unique hashes*). By sharing these pseudo-anonymous *hashes* and digital identifiers across a computer network, blockchain ensures their resilience to change: any modification of the information would change the associated sum, and would be rejected by the validators of said blockchain network.

[920] Art. 1367 of the French Civil Code: "[...] It expresses consent to the obligations arising from this deed. When affixed by a public official, it confers authenticity on the deed. [...] ".

[921] Art. 1367 of the Civil Code: "The signature required to perfect a legal act identifies its author. It manifests his consent to the obligations arising from this act. When it is electronic, it consists of the use of a reliable identification process guaranteeing its link with the act to which it is attached. The reliability of this process is presumed until proven otherwise.

[922] Art. 1367 of the Civil Code: "[...] When it is electronic, it consists of the use of a reliable identification process guaranteeing its link with the act to which it is attached. The reliability of this process is presumed, in the absence of proof to the contrary, when the electronic signature is created, the identity of the signatory assured and the integrity of the document guaranteed [...]".

[923] Art. 10 of the Civil Code: "Everyone is obliged to cooperate with justice in order to establish the truth. [...] ".

automated computer witnesses[924] . It is important to emphasize that a blockchain can be used to certify the integrity of data and information, but not its veracity, which would require formal and perfect verification, including by a legal professional as mentioned above. In this sense, the reality of the fact reported on a blockchain depends ex ante on the person who registered it, i.e. the person who deposits it on the b l o c k c h a i n . We can conclude from this that the probative value that a judge will grant to information registered in a blockchain will ultimately depend on the conditions of its deposit, registration and restitution[925] . More specifically with regard to the attributes of decentralized digital identity (IND) studied in the second part[926] , the use of a self-sovereign digital identity solution (INAS)[927] does not appear to be able to guarantee the production of perfect evidence due to the principle of autonomy of evidence. According to this principle, the validity of evidence cannot depend on non-verifiable elements, even if these elements are assumed by a digital community as is the case for an INAS, which is not sufficient to guarantee this principle of autonomy in legal terms. Consequently, a verifiable attestation can be considered as the beginning of written evidence under French civil law, provided that the identity of the issuer is clearly established. In the short term, it is likely that self-sovereign identity will become hybrid[928] , i.e. that it will become partially centralized by identity providers. This mixed evolution (2.0 and 3.0) aims to ensure that cryptographic proof mechanisms such as verifiable credentials (VCs)[929] and decentralized identifiers (DIDs)[930] comply with national and EU digital identity schemes, under eIDAS-1 and eIDAS-2[931] .

In order to answer our initial question, we must first emphasize the interest and technical relevance of an open blockchain in cases where evidence is free: blockchain evidence constitutes an electronic medium that is admissible until proven otherwise. Nevertheless, this tool for evidence will not become a probative Holy Grail without appropriate and dedicated legislative amendments.

---

[924] Reference is made to the numerous computers/validators of the transaction blocks of these decentralized networks, which in a certain sense each *bear witness to* the transactions communicated to them, until together they form a *common* and *consensual testimony, i*.e. form a *consensus* concerning the legitimate transactions to be recorded or rejected from said network. It is important to stress that each blockchain and each consensus may vary, which would call into question this very interpretation.

[925] Reference is made to the differences in restitution that may exist depending on the type of public, private or hybrid blockchain in question. These technological variants, as well as the context in which they are used, can thus lead to significant changes in the techniques for recording, verifying and restituting information anchored on said blockchain.

[926] See *below*, II, Title I, Chap. 1

[927] *See infra*, II, Title I, 1.4

[928] Self-Sovereign Identity (INAS) advocates total management by the user of his or her identity, including on-boarding and prior digital identification of a person. INAS is thus particularly disruptive and will be confronted - in the short to medium term - with centralized digital identity schemes: it will therefore have to conform to them, and so the concept of purely decentralized *Self Sovereign Identity - SSI* - will give way to the concept of distributed identity (rather hybrid, i.e. both 2.0 and 3.0), favored in this research.

[929] See *infra*, II, Title 1, 1.3.1.2.

[930] V*, infra*, II, Title 1, 1.3.1.1

[931] V*, infra,* II, Title 1, 2.1.1

In the hope that such an awareness will recur[932] , would legislative intervention be desirable and relevant to recognize the evidentiary potential of information anchored on a public blockchain? It should be noted that the legislator has already intervened in this sense for the ownership of unlisted company securities, resulting from an ordinance of December 8, 2017[933] and a decree of December 24, 2018[934] where it adopted a technical reform consisting of facilitating the proof of title account recorded on a blockchain. Among other things, this reform made it possible to consider blockchain technology as a whole as a technical tool at the service of proof of ownership of securities, without modifying the legal regime of ownership of securities in force. Thanks to this legislative intervention, blockchain has the same evidential value as a paper register when it comes to ownership of unlisted securities (and not for other types of non-financial blockchain transactions). In this sense, the legislator's technology-agnostic approach perhaps explains the current status quo regarding the law of evidence in the light of blockchain technology: in order not to breach this technological neutrality, the legislator prefers to observe whether the technological adoption of blockchain will rather concern public, private or hybrid registers (bearing in mind that the eIDAS-2 Regulation decides in favor of private and hybrid blockchains, as suggested below)[935] . The French legislator has therefore not decided in favor of precise specifications and technical guarantees for either of these technological variants. In fact, the Ministry of Justice has decided to

- behind the scenes - not to legislate to attribute probative value to blockchain evidence. As is often the case, the latter favors the formation of jurisprudence as a source of law, which implies that professionals in the judicial sector are unfamiliar with this technology yet at the service of evidence. Some countries, such as Monaco (2017)[936] and a few years later Italy (2019)[937] , have already legislated on this subject with a view to fostering innovation while accepting the full evidentiary potential inherent in blockchain technologies (admittedly relative in its public versions but compliant with the law of evidence in its hybrid or private versions). Since September 2022, a new Italian decree has made it possible - in coordination with companies and public or private research centers - to apply for subsidies (total envelope of 45 million euros) to carry out research and technological innovation projects concerning blockchain technology[938] . In these respects, the aim is to work towards a European harmonization of evidence using blockchain technology, as more and more legal experts seem to be progressively supporting: "*as soon as there is a*

[932] Reference is made to the legislative foresight shown by the French legislator in the Act of March 13, 2000, adapting the law of evidence to information technology. Indeed, the legislator was able to anticipate the technical importance of digital signatures and, more generally, of digital technology in our daily lives.
[933] Ordonnance n°2016-520 of April 28, 2016 (art. L.223-12 & L.223-13 of the CMF), in application of the Macron law of August 6, 2015, gives blockchain technology its first legal recognition in French law, available online
[934] Décret n°2018-1225 portant diverses mesures relatives aux contrats de la commande publique.
[935] See *infra*, II, Title 1, 2.1.1.1.a
[936] The State of Monaco recognizes a presumption of reliability of any registration on a blockchain.
[937] Law no. 12/19 of January 11, 2019 on the support and simplification of businesses and public administration, which came into force in Italy on February 13, 2019. It reinforced the legally binding nature of electronic time stamping carried out using blockchain technologies. V. BARBET-MASSIN Alice, *in Revue Lamy droit de l'immatériel* (Wolters Kluwer), n°157, March 2019, pp. 40-43.
[938] "Blockchain e intelligenza artificiale: da settembre gli incentivi", July 5, 2022, in *mise.gov.it*. Available online

cryptographic protocol, the proof is considered advanced. But until a French or European legislator says that proof by blockchain is equivalent to advanced proof or simple proof, we'll remain in the dark."[939] .

2.9 Universal online identity 3.0 with Proof of Humanity (PoH)

On April 16, 2021, Kleros embarked on the self-sovereign digital identity (INAS) path, explored below[940] , with the launch of another 3.0 project called "*Proof of Humanity - PoH*". This is a "*system combining trust networks* (...) *and conflict resolution to create a Sybil-proof list of humans*"[941] . The Proof of Humanity concept aims to establish a reliable system of digital proofs of existence for users by combining social verification and video submission on a decentralized platform. Kleros, which has developed expertise in decentralized digital justice as mentioned, is using this expertise to offer a decentralized digital proof-of-identity solution to all Internet users. The problem of identity verification is a common issue in the crypto-asset ecosystem and on the Internet, as some malicious users can create multiple accounts and digital wallets pseudo-anonymously in an attempt to receive rewards multiple times, influence votes, write fake reviews, etc. Proof of Humanity addresses this problem ("Sybil")[942] by offering a distributed digital identity verification (IND)[943] , reliable and secure, which users can use to authenticate themselves to digital third-party services such as social networks, blogs and financial platforms. This solution thus attempts to solve the day-to-day difficulty that individuals have in proving their identity online. PoH is still in its infancy, but several use cases have already been envisaged. Firstly (i), the implementation of a universal income in crypto-assets is proposed. Once a person has deposited his or her identity on the PoH platform and it has been verified by other trusted users, he or she receives the right to receive a universal income in the form of a digital token, the "*Universal Basic Income - UBI*". Thanks to this solution, deployed in 2021, every Internet user whose "humanity" is verified receives 1 UBI per hour (i.e. 720 UBI per month, equivalent to around 108 euros per month as of 2021). Although UBIs can be exchanged, their value and price are still in the exploratory phase and can therefore vary considerably. This distribution of (crypto)income is free of charge and partially decentralized. In a second phase (ii), the PoH platform would make it possible to check the creditworthiness of a crypto-investor. Indeed, many users and professionals in the crypto-economy currently resort to the use of

[939] MAGNIER Véronique, "L'Édition de l'université Paris-Saclay été 2021", éd. 2021, issue 16, p. 10. Available online.
[940] See *infra,* II, Title I, 1.4
[941] Kleros, "Welcome to Proof of Humanity", 2021, YouTube, available at
[942] *See* previous section, also Appendix 6, Focus 1.
[943] Any Internet user can already register on the PoH website and platform in order to obtain a form of self-sovereign digital identity and receive a universal (crypto)income. To do so, visit the following address

loans in crypto-assets for investment or speculation purposes (to overexpose oneself to the market). These highly risky crypto-asset loans are generally offered by specialized exchange platforms[944] . As explained in the previous sections, these platforms have identification obligations, but also wish to systematically check that their customers and users are solvent. Consequently, PoH enables these exchanges and trading platforms to ensure that a person is who they claim to be (civil identity verification) and that they actually own what they claim to own (solvency verification). Finally (iii), many online communities claim their digital allegiances, a need for social recognition that is very much in vogue in the crypto-economy, where projects, communities and crypto-assets of different natures and reliability abound. To combat Sybil attacks, PoH enables project owners to engage verified[945] and unique user communities in a way that is supposedly more targeted and effective (than the digital identity verification 2.0 studied previously). PoH's experimental project is therefore based on the vocation of a high degree of decentralization, as well as on the desire to open up and emancipate people's digital identity, by offering a universally accessible identity on the Internet. Finally, this 3.0 platform for aggregating digital identities gradually opens the door to certain digital rights, such as the universal income mentioned above, or the right to vote in the governance of this protocol, which aims to become a digital commons. In theory, PoH is managed directly by its users via a DAO that respects the principle of democracy without a trusted third party: "*one person, one vote*"[946] . In short, PoH represents one of the first IT solutions - behind "DID4ALL" initiated in 2019[947] - to generate and verify proofs of digital existence in a distributed way and at the service of Internet users and their digital rights[948] . PoH is an accessible and open system that relies on transparency as well as on a supposedly growing community involvement of its users. The prospective potential of this system can be summarized as follows:

[944] It is important to differentiate between centralized and decentralized platforms. The former simply act as centralized financial intermediaries (PSCA), while the latter operate autonomously and partially decentralized (DeFi), thanks to the use of technologies such as AECs and DAOs.

[945] Based on a new technological layer called "*token curated registry"* (*TCR)*. Conceptually, the *TCR* is an online registry of humans (information such as photos, videos, biometric data such as voice, etc.) enabling it to resist *Sybil* attacks. Computerized, to register on a *decentralized list*, an applicant buys the native token ("UBI Tokens") and submits an online request. Token holders can contest an application (thanks to Kleros) if they feel it doesn't belong on the list. When a challenge is launched, token holders can vote to accept or reject the application (their vote is proportional to the number of tokens they own). If the application is rejected, the deposit is lost: it is shared between the auditor who initiated the audit request and the token-holders who voted for rejection. If the request is accepted, the above principle is reversed.

[946] Available since 2022, this DAO defines the technical and social orientations of this solution. See how it works at

[947] See *infra,* II, Title2, 2.1

[948] See *infra*, II, Title 1, 2.2.

Key success factors (KSF) for PoH	Short term	Medium-term	Long term
Legal compliance and political recognition	×	× or ~	~
Recognition and social adoption[949]	✓ or ~	✓ or ~	✓
Recognition and computer adoption (Ethereum[950] , UBI/TCR, DAO)	~	✓ or ~	✓

This prospective picture suggests that legal and political recognition in the medium term would be essential to foster the social and IT adoption of the self-sovereign digital identity solution (INAS) proposed by PoH. However, it should be noted that PoH currently has only partial IT recognition and no legal recognition due to its probable non-compliance with multiple provisions of the RGPD, TFR and eIDAS Regulations, as well as the DSA and DMA mentioned upstream. Although PoH theoretically makes it possible to provide proof of digital existence for every individual, in practice this remains a phygital utopia compared to other hybrid (2.0) digital identity systems framed by law or by a public authority (*v.* project "DID4ALL"[951]). For the time being, PoH is an immature IT system, subject to numerous economic and IT dependencies, which could lead to flaws, as was observed in 2022 for its neighboring Kleros project[952] . In this respect, if the IT challenges remain legion in 2021 for such a digital identity 3.0 solution, it has to be said that the interweaving of the Kleros solution and PoH is IT and above all commercially relevant, even if it is largely subject to questioning and interpretation on the legal level, if only on the (crypto)economic relevance of mixing self-sovereign digital identities (INAS) with decentralized digital justice (Kleros).

[949] On March 15, 2023, 18,322 Internet users were registered and verified on the PoH platform, accessible at the following address. Since its launch, the majority of PoH users have been in South America.
[950] V. Appendix 6, Focus 2.
[951] See *infra,* II, Title2, 2.1
[952] *Op. cit.* "DAOs are not corporations: where decentralization in autonomous organizations matters", accessed September 20, 2022 at "The Court's incentive-based decision-making process is, to all appearances, corrupted by a single developer who had too large an economic interest to the tune of 25% in the courts [Kleros]".

Conclusion of the first part

Our study of identity shows that this notion has been defined in numerous ways in the social sciences. Here observed and relatively circumscribed through its philosophical, legal and social fields, identity nevertheless remains ductile and more often than not elusive for its observers of average attention. While the law helps to establish certain essential facets of personal identity, identity must in fact be systematically (re)contextualized in order to be understood in terms of the objects and subjects it deals with as much as those that feed into it. By understanding the chronology of computing 1.0, then online services and digital identity systems 2.0, we are able to determine the technological and social progress achieved, as well as certain IT and legal challenges to be met, and finally certain latest-generation technological opportunities and needs linked to the emergence of 3.0 governance systems, supposedly more transparent than before. A semantic and segmented analysis of public, private and hybrid blockchain technologies, as well as their respective main technological bricks, highlights new IT foundations, with regard to an Internet presumed to be more sovereign, secure and respectful of Internet users' rights. Against this backdrop, a number of proposed European regulations - at the time of writing voted but not promulgated - are gradually focusing on this revisited phenomenon of IT decentralization 3.0. It's up to all players in society, including lawyers, institutions and governments, to patiently, pragmatically and expertly take on board the issues, promises and challenges linked to these new technologies, in order to at least partially reinvent some of our phygital governance models, which sometimes lack online transparency.

II/ Blockchain and decentralized identity at the service of law and identity

Title 1: The hypothesis of a universal cryptographic identity as a source of strengthened rights

Chapter 1: The emergence of a new, decentralized, universal identity for humanity

1.1 Contextual and semantic introduction to a third-generation digital identity

As a reminder, the notion of identity has never been so central to our societies, due to the fact that over a billion people today find it difficult to prove their legal existence[953] . As we have seen, identity documents are becoming digital, and are gradually giving rise to a regal online identity. Personal identity is made up of an infinite number of fixed (eye color, voice[954]) and variable (hair color) personal attributes, as well as roots (patrimonial first and last names) and extensions (professional experience, diplomas). In 2016, the Pan-Canadian Confidence Framework (PCF) described a distinction between identities called "*foundational"* and those called "foundational".
"[955] . In today's 2.0 digital identities, these innumerable attributes and identity data are generally under the control of organizations and servers external to the individual to whom they refer. As a result, digital identity 2.0 regularly raises a variety of issues, because it is fragmented between different organizations, often private, not interoperable or accessible, costly and complex to secure. In some cases, its management is opaque, to the detriment of users and their personal data, which is sometimes marketed with impunity online or offline. The challenge of a trusted digital identity, partly based on certain blockchain technologies, is emerging and opening up to businesses, citizens and governments alike. In an unprecedented way, it enables identity transactions to be given a legal and cryptographic value, which actors will legitimately trust, once they are initially derived from official identity documents. More than just a technology in a historic market, it represents a new techno-social concept for both the identity of individuals and legal entities, and for the Internet of Connected Objects (IoT)[956] . Decentralized identity does not yet have a stable definition, but rather a set of principles and concepts. In 2022, fifty industry experts seem unanimous in their view that it will develop faster than the Internet.

---

[953] DESAY Vyjayanti, DIOFASI Anna, "The global identification challenge: Who are the 1 billion people without proof of identity? World Bank Blogs", April 25, 2018, available at.
[954] Cour d'appel de Paris, May 28, 2014, RG n°12/20952, there are few rulings concerning voice protection, an
In this case, the "*personality attribute*" invoked as freedom of expression to justify the recording of a tax audit (aff. David Guetta who used a website offering to synthesize a person's voice).
[955] MONTANA Kent, "Digital identity in the 21ème century", June 25, 2021, Digital trust series: part one | Digital identity, available at
[956] See *infra*, II, Title 2, 1.6

in its early days[957] , although some authors distinguish it from the notion of Self-Sovereign Digital Identity (SDI) studied below[958] , a position echoed in this study. This latter Anglo-Saxon concept is ambivalently referred to as "*Self-Sovereign Identity" (SSI)* or, more generally, "*Decentralized Identity*" (hereinafter IND). However, there is a subtle distinction between these two terms, as confirmed in 2021 by a group of European researchers[959] . In concrete terms, INAS offers a degree of user control that goes further than the generic notion of Decentralized Digital Identity (IND), to which it belongs. While it's agreed that INAS necessarily incorporates the IT operation of a decentralized digital identity, the latter is not systematically an INAS. This distinction is also necessary to understand the link between INAS and a universal digital identity proof system[960] . In this respect, it is important not to give people too much freedom over their root identity attributes - initially a purely regal prerogative - at the risk of their being partially abused or misused. The following sections explore how decentralized identity proposes a new arrangement in which the user is sovereign, from the online creation of his or her digital identity attributes to their sharing with third parties[961] . IND thus contributes directly to reducing the boundary between 2.0 and 3.0 digital identity solutions, by giving probabilistic data a deterministic character, as the data is 'cryptographically' framed by a trusted third party, while offering autonomy to its users. With IND, individuals can choose what information can or cannot be made publicly known by public or private third parties and online services. The granularity of this information and digital attributes varies according to each social context. While an individual may wish to provide only the minimum information required to a public authority, he or she may conversely decide to share very personal details with certain social circles of his or her choice, family or friends. In specific cases (INAS), the user may need different profiles or social circles to present trusted information to online services. By

[957] PREUKSCHAT Alex, REED Drummond, presentation 2022, "The Future of Self-Sovereign Identity (SSI)", YouTube video, available at, *see* also "Self-Sovereign Identity Decentralized digital identity and verifiable credentials", book published in 2021, in *Manning Publications*.

[958] Although many researchers use the acronym "*SSI"* to refer to the concept of decentralized identity, we discard the use of this acronym already used by players in the IT sector to designate *Information Systems Security (ISS)*. What's more, decentralized identity and self-sovereign identity differ slightly in terms of the degree of control by the user according to the European Union Blockchain Observatory and Forum's report "Blockchain and Digital Identity", published May 2, 2019, accessed online 04/10/2021, freely translated from English, p.14: "It is possible to go further in decentralizing identity by giving users control not only of their identifiers but also of the data associated with them. This is at the heart of what is known as self-sovereign identity (SSI)", and see *infra* II, Title 1, chap. 1, 1.4.

[959] SEDLMEIR Johannes, SMETHURST Reilly, RIEGER Alexander, FRIDGEN Gilbert, "Digital Identities and Verifiable Credentials", 2021, translated from English, "Self-sovereign identity (SSI) is a contested name that is often used to promote various decentralized digital identity projects", accessed online 08/10/2021, p.4.

[960] See *supra,* I, Title 2, 2.9, see also *infra*, Part 2, Title 2, chap. 2, 2.1.

[961] Trust Over IP Foundation, check out the following tutorial to understand and visualize this new digital identity model.

As a result, the possibility of a third-generation digital identity, computer-verifiable and distributed, opens up unprecedented new phygital and societal possibilities.

1.2 IT and conceptual definition of decentralized digital identity (IND)

Decentralized digital identity (IND) proposes a reinvention of the way in which individuals' online identities are conceived, generated and exploited. This new computing paradigm places the user at the center of the identity management model, while eliminating the need for a trusted third party to adiministrate him or her. In a way unheard of in the Internet age, a user now has the opportunity to become an actor, and no longer simply a spectator, of his or her own digital existence. In practice, decentralized identity enables users to possess, on a single digital application, some of the digital attributes that make up all or part of their identity (proof of majority or nationality, diplomas and/or professional qualifications, insurance or financial certificates). The user thus owns all or part of his or her identity fragments directly on a new-generation mobile application: a decentralized digital identity wallet (defined by "PIND")[962] . This mobile or web application can be defined as a digital dashboard providing a real-time overview of a person's identity data, which can be controlled via this 2.0 or 3.0 interface. They can then receive or issue[963] digital certificates and attributes directly from this application, and share them online or offline with selected third parties. In IT, this latest-generation identity scheme, described in detail below, enables users to manage their digital identities using unique identifiers called "decentralized identifiers (DIDs)"[964] , which are cryptographically associated with "verifiable credentials (VCs)"[965] , also studied below. These few definitions raise a number of questions, not least those concerning the IT specificities involved in these new-generation exchanges of identity attributes. What are the new opportunities, challenges and IT and social consequences of using IND and/or INAS? How will people's rights be respected, framed and impacted in the digital spheres of civil society? Decentralized digital identity is a concept first raised in 2012[966] , followed by a major acceleration of interest in and adoption of these new IT standards in the private sector and from 2017 onwards. By 2019, nearly 170

[962] *See infra*, Part II, Title 1, chap. 1, 1.3.1.3.
[963] *See infra*, Part II, Title 1, chap. 1, 1.3.1.2.
[964] Translated from Decentralized Identity (DID), which stands for "Permanent, unique identifiers that do not require a centralized registration authority and are often cryptographically generated and/or stored" according to the *Decentralized Identity Founfation (DIF)*. However, many, but not all, *DID* methods use blockchain technology or other types of decentralized/distributed networks. See *infra*, II, Title 1, 1.3.1.1.
[965] See *infra*, Part II, Title 1, chap. 1, 1.3.1.2, see also *op. cit*. 2021, hal-03398096
[966] STOKKINK Quinten. POUWELSE Johan, "Deployment of a blockchain-based self-sovereign identity" CoRR, 2018, available online.

Decentralized digital identity (IND) and self-sovereign identity (INAS) solutions have been identified according to a study by the French Ministry of the Interior[967] , and around 90% of existing "*Self-Sovereign Identity - SSI*" solutions have been implemented within a blockchain infrastructure to date. Because the user has theoretical partial (IND) or total (INAS) control over his or her 3.0 identity attributes, a practice explored in the next paragraphs of this section, it enables new online interactions. In simplified terms, it systematically involves the presence of (i) a sender, (ii) a user and (iii) a verifier (*see* following diagrams). These interactions are such that the first transmits one or more identity attributes, the second receives them and the last verifies them. These roles can be combined by the same entity, depending on the identity use case in question.

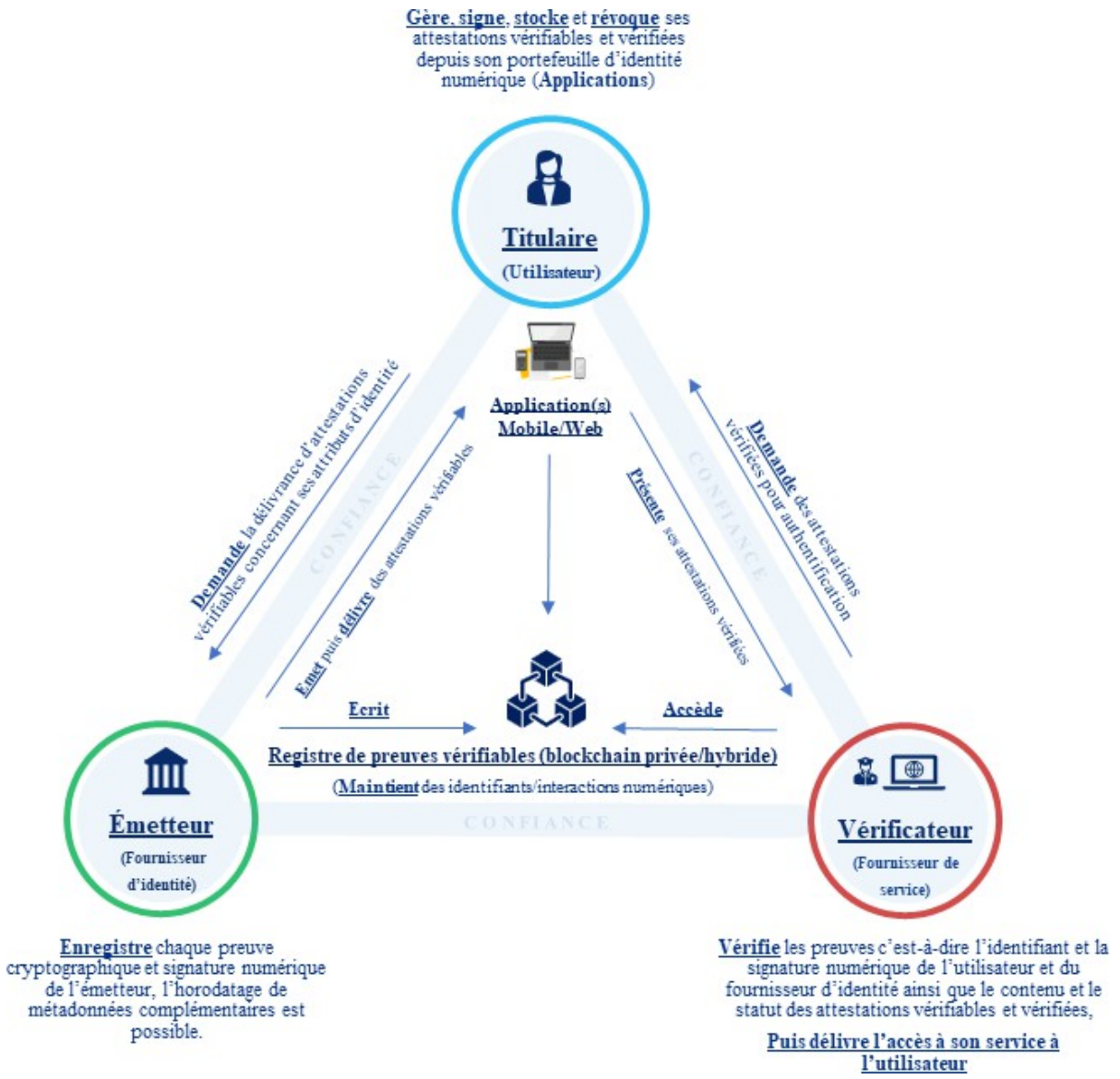
Individuals routinely use certificates to establish their identity on a day-to-day basis. These documents can take the form of passports, driving licenses, certifications, diplomas, insurance cards or medical certificates. Typically, these proofs of identity are physical, made of paper or plastic. By applying a digital decentralization approach to a person's identity, their physical credentials can be transformed into verifiable digital credentials[968] . To do this, they need to be converted into a standardized digital format and stored locally on the user's phone or remotely on a server belonging to a trusted third party (public institutions, certified private companies). These Verifiable Credentials (VCs), discussed below, represent standardized digital certificates that enable their holders to share information online autonomously and securely. The notion of IT standardization indicates that there is a compliant method for programming a verifiable attestation, a mechanism currently being standardized by the
The "World Wide Web Consortium - W3C"[969] so that identity and service providers in this 3.0 ecosystem can use common, interoperable IT standards specifically dedicated to the tools mobilized by decentralized digital identity. By associating verifiable attestations from Internet users with recognized authorities such as governments or private companies, users benefit from digital counterparts[970] that extend their regal and physical attestations. Indeed, thanks to a verifiable attestation, a national identity card (CNI) has a digital twin that is just as admissible online and offline as its palpable, official version. Once generated, a person's verifiable attestations can be shared by the user from their phone, computer or even browser, thanks to a

[967] *Op. cit.* HENNEBERT Christine, al, "Blockchain et identification numérique - Restitution des ateliers du groupe de travail 'blockchain et identité'", 2020, available at
[968] The notion of verifiable attestation does not yet have a unanimous translation in French. See *infra*, II, Title 1, 1.3.1.2.
[969] Verifiable credentials are standardized by the World Wide Web Consortium (W3C), a standard available at this address. The W3C is made up of over 450 organizations invested in W3C's decentralized identifiers and verifiable attestations to ensure a more decentralized, privacy-friendly and consent-based data-sharing ecosystem.
[970] While the integrity of the information contained in a verifiable certificate can be verified, its authenticity cannot. Although the auditor is obliged to trust the issuer of the attestation, he does not need to contact the issuer directly to verify the information, as long as he trusts the issuer.

specific web extension[971] - by e-mail, SMS, QR code or Bluetooth - in order to prove certain root or extended information attached to one's identity. The cryptography involved in these new 3.0 digital standards plays a central role in the technical realization of a distributed/decentralized digital identity[972] . Its implementations use cryptographic proofs - persistent or disposable digital fingerprints - theoretically unforgeable thanks to blockchain technologies, for the purpose of providing mathematical certainty regarding the link between an individual and his or her digital data. However, decentralized digital identity does not necessarily require blockchain technology as the underlying digital infrastructure. In fact, the technical standards used enable all types of entity to be provided with verifiable attestations that are autonomous and shareable, regardless of the digital registry on which they evolve (centralized, distributed or decentralized servers). Yet pairing these new standards with blockchain technology is undeniably a wise move. The intrinsic advantages[973] offered by a decentralized blockchain infrastructure are naturally transposed to these standards, as long as they are based on the latter. In fact, many decentralized identity projects are currently based on blockchain technologies, which are in fact more or less immutable and decentralized from an IT point of view.

[971] Wikipedia contributors, "Plugin", 2022, available at
[972] From now on, one or the other of these two terms will be used to designate the same concept - that of IND - while signifying a difference in degree concerning the level of decentralization in question.
[973] Reference is made to the characteristics and advantages of blockchain technologies: immutability, speed, security, accessibility and pseudonymity of registry transactions.

1.2.1 The triangle of trust in decentralized digital identity



The "triangle of trust" is a theoretical concept specific to decentralized identity, providing a visual illustration of some of its main components and digital interactions. This diagram - which is not exhaustive from an IT point of view - places the identity holder at the center of information exchanges concerning him or her. Three entities have one or more roles[974] , participating in the end-to-end exchange of encrypted information[975] : (i) a sender, (ii) a holder/user and (iii) a verifier. The relationship between these roles is described in this triangle of trust:

[974] In theory, all roles can take the place of another role, meaning that an issuer can also be a holder or a verifier. In practice, an individual as a holder might not be able to play the role of an issuer since some verifiable proof registries (public blockchains) do not allow individuals to write down their decentralized identifiers (DIDs) for RGPD compliance reasons.
[975] The term "encrypt" is preferred to "crypt", according to the online site *BlogChiffrer.info*, available online at

(i) The issuer of identity information, as a trusted third party, provides - via a centralized or decentralized electronic registry - proof of the validity of the verifiable assertion issued to the holder, by electronically signing it with his or her private cryptographic key. The issuer's public key can be stored in a centralized verifiable data register (server) or in a decentralized register (blockchain). This enables each party to independently verify the accuracy and validity of the verifiable certificates issued. Once the holder has signed the certificate cryptographically, his or her Verifiable Certificate (VC) becomes a Verified Certificate (VP), i.e. with the same value as a handwritten paper certificate, as described below. Because the issuer sends the holder a signed version of the latter attestation[976] , it can be verified by a recognized entity (state) and/or verified online by any third party (online services).

(ii) Once received by the holder/user, the information can be stored directly on any connected machine or digital wallet (PIND) as already mentioned, to receive, store and share its verifiable (VC) and verified (VP) certificates.

(iii) The verification process is initiated by the computer system of a verifying organization, which accepts the implementation of decentralized identifiers (DIDs) and the sending of verifiable and/or verified attestations to a holder who will decide - or not - to send it to the verifier to prove his or her identity attributes. The verifiable data register (blockchain) enables the verifier to ensure automatically and in real time that each proof of identity provided by the holder has been previously validated by the issuer.

This diagram shows that every interaction between these three entities is, in principle, transparent and verifiable, i.e. trusted. These digital interaction mechanisms are new and, for the time being, are being deployed on non-industrial, i.e. mainly experimental, scales. Ultimately, while one of the main advantages of distributed digital identity lies in the verifiability of the information presented between the aforementioned entities, trust relies first and foremost on a trusted issuer, generally certified by the State or its public institutions. Thus, decentralized identity is in fact a hybrid, and does not currently tend towards a significant degree of decentralization, as advocated by the self-sovereign identity model (INAS) discussed below.

[976] VCs are signed by their issuer. The signature and therefore the declaration can be verified using blockchain technology or other adjacent cryptographic mechanisms.

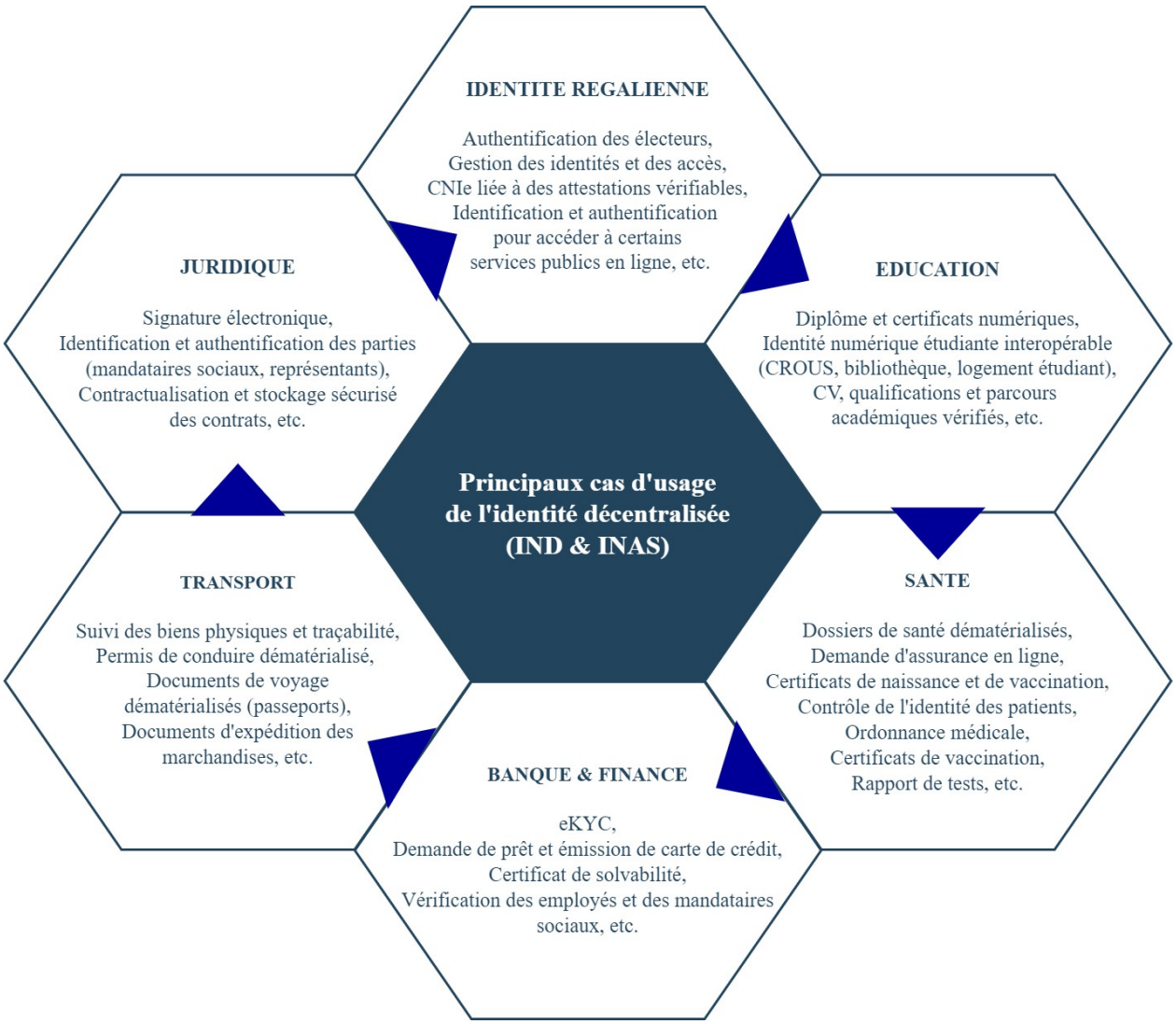
1.2.2 Ten founding principles for a decentralized identity that generates trust

To ensure that the concept and methods used by decentralized digital identity inspire confidence, one of its founding fathers and IT programmer, Christopher Allen, has proposed ten principles to be respected by any entity wishing to provide IND solutions[977] , namely (i) the importance of placing the user at the center of the digital identity scheme, (ii) giving him control over his digital identity, (iii) guaranteeing that the user has access to his own data, (iv) ensuring the traceability of this data, (v) guaranteeing the durability of evidence of information exchanged, (vi) enabling the portability and (vii) the interoperability of data, (viii) obtaining the systematic consent of the user, (ix) minimizing the disclosure of his data and (x) protecting it. Enunciated in April 2016, these ten principles reflect Christopher Allen's personal vision of distributed digital identity. Several of these ten principles are probably derived from the values and principles of the RGPD adopted on April 14, 2016 as studied upstream[978] . Once implemented by a distributed identity solution, these ten principles therefore propose a form of compliance by design with the RGPD, as some specialists seem to confirm[979] . When interacting with a digital identity, trust is paramount, whether centralized (dependent) or decentralized (independent). Trust requires reliable, sustainable social and institutional structures, backed up by legal certainty. Service providers must be able to have confidence in the source of a distributed identity, necessarily linked to the regal and civil identity of individuals. The State thus guarantees the identity of individuals, and digital identity must continue to rely on this fundamental, legal identity, while leaving individuals free to use pseudonyms with a self-sovereign digital identity (INAS). In the case of a distributed digital identity, transparent cryptographic underpinnings controlled directly by the individuals concerned can provide effective legal recourse in the event of identity theft[980] or revocation of digital credentials[981] . It is also important to have confidence in the traceability of interactions and every online action, which has become essential for law enforcement in the fight against crime or terrorism. The minimization or compartmentalization of digital identity data could become a new fundamental IT security and standard, empowered incidentally by the IND. Minimization discourages and limits the scope for malicious and fraudulent use of personal data. Although this principle of minimizing identity attributes contradicts certain social uses specific to crypto-economy and open blockchains, this research supports this idea for the advent of a digital identity of

[977] ALLEN Christopher, "The path to self-sovereign identity - Ten principle of self-sovereign identity", April 25, 2016, available on his personal blog at.
[978] See *supra*, I, Title 2, chap. 2, 2.4.
[979] Société Archipels, "Why the ISS is compatible with the RGPD?", February 16, 2022. Available at
[980] See *supra*, Part I, Title 2, chap. 1, 1.4.1.1.
[981] The revocation of an attestation means its cryptographic cancellation, a new feature that is possible by design in every verifiable attestation.

the latest generation. These fundamental principles for the future of decentralized digital identity may seem difficult to reconcile for each of the three entities in the triangle of trust, so it's up to each player involved in this value chain to guarantee them and not leave this objective to be achieved solely by the legislative and executive powers.

1.2.3 Sectoral uses and applications of decentralized identity



The need to use an IND is directly linked to the requirements of industries that need systematic, online identification of their users. These industries are potentially infinite, as illustrated in the diagram above, including the public sector (digitization of driving licenses and passports), the private sector (digitization of business cards), the financial sector (transfer of assets), the banking sector (on-boarding and identification processes of

customers), the insurance sector (proof of claims), education (diplomas, internship certificates), the health sector (vaccination certificates) and the legal sector as studied earlier (document storage and electronic signatures). In general terms, the use of verifiable identity credentials (VCs) and decentralized digital identity portfolios (PINDs), studied below, can have a considerable impact on e-commerce check-in and check-out processes. For example, a user who is not registered on a commercial website could place an order simply by using a digital wallet containing his or her identity attributes. By scanning a QR code, he could confirm the disclosure of certain identity information such as his address or age directly contained in verifiable identity certificates (VCs). This method significantly reduces the use of digital IDs and passwords, or even eliminates them altogether in some cases, which is a practical advantage over the 2.0 digital identity currently in use. An example commonly used since the advent of the Internet concerns online messaging, now massive, which could also benefit from IND to offer greater interoperability, security and intelligence between multiple online services. By enabling users to take control of their digital identity, decentralized digital identity helps them to regain control of their digital destiny. This new model of 'augmented' identity, based on transparent digital trust, represents a new opportunity for society. This new digital identity
3.0 can also be applied to the authentication of digital objects, as suggested below, making all online or offline processes requiring proof of one or more qualities via identity attributes more transparent and reliable. In the medium term, decentralized identity is likely to be a hybrid, comprising digital infrastructures and technological bricks that are both centralized and decentralized - in other words, distributed. To be widely adopted, it will need to be supported by a technical, economic, political and legal consensus. An amendment to the European eIDAS Regulation[982] , discussed below, partially describes some possible use cases for the IND, such as the ability of citizens and residents to prove they hold a valid driving license, and the competent authorities to verify and trust this phygital information. In the longer term, it seems that the self-sovereign digital identities (INAS) also detailed below will find their applications in some of the more decentralized universes of Web 3.0. Ultimately, the fundamental needs of the digital identity market focus on the security of registration, management and identification methods, as well as on the IT and legal confidence of the solutions made available. It seems essential to offer identification systems and schemes that all users can trust, while respecting personal data rights, the aforementioned right to pseudo-anonymity, and consent by design and systematically.

[982] See *infra*, II, Title 1, 2.1.1.1.a

1.2.4 Theoretical issues and benefits

The benefits of distributed digital identity compared to conventional 2.0 identity management methods already studied are numerous and can be summarized through the prism of the user (i) and then that of organizations (ii). For the user (i), (distributed) digital identity will become easier to use. Once deployed, a verifiable credential (VC) can be easily shared between different Internet services for authentication purposes. The user no longer needs a password for each service, and digital identity becomes consented, portable and interoperable from one online service to another. Traditional mobile and web applications will be able to connect to this distributed system(s) to request permission to access the user's identity. In this way, it is at the user's discretion to accept and share certain desired information, and to choose when to grant or revoke access to identity data previously accessible to third parties. This new cryptographic selectivity feature will benefit Internet users and help curb the undue commercialization of their personal data on the Internet. Given its inherent respect for privacy and personal data[983] distributed identity makes it less likely that third-party digital services will aggregate data and abuse users' confidentiality. IND is also more secure than centralized digital identity, since the user alone controls access to and sharing of his or her identity attributes via the decentralized digital identity wallet (PIND) described below. This makes identity theft more difficult, a boon for the 8% of French people who say they have been victims of identity theft in the last ten years[984] . For its users, however, decentralized identity implies a less intuitive online browsing experience, but it will help to reduce the number of victims of digital phishing for both individuals and legal entities[985] . In the user's PIND, it is possible to store different types of documents such as national identity cards, invoices, certificates, permits and authorizations. Thanks to this functionality, users will in future be able to detect each Verified Certificate (VC) and automatically fill in online forms on behalf of other users, thus considerably reducing their workload and improving user convenience. For organizations (ii), a decentralized identity system confers security and cryptographic reliability on stored information and interactions with other entities. Distributed digital identity enables organizations to provide their users with a new, simple, secure and universal means of authentication, and to efficiently automate certain tasks.

---

[983] The W3C's technical standards are based on the "10 principles of self-sovereign identity" set out above. "Existence, control, access, transparency, durability, portability, interoperability, consent, minimization, protection" [984] CSA, "Les Français et la criminalité identitaire", survey, in *Fellowes*, Oct. 2012, p.4 and see *supra*, Part I, Title 2, Chap. 1, 1.4.1.1
[985] This can result in a reduction in the number of "*phishing*" victims, since the user has only one reliable channel of communication with a company, instead of receiving e-mails from a trusted source, but actually from a fraudulent third party.

internal or external processes requiring increased digital trust. By way of illustration[986] , in the event of injustice or digital censorship of a user without legitimate grounds by an online service, acts such as unjustified censorship or unjustified closure of business accounts would be easily and technically traceable. With IND, certain infrastructure costs are also shared between companies, public institutions and any other organizations involved in the infrastructure, often a common underlying closed blockchain. As a result, a new era of collaboration is emerging for organizations that can benefit from the same distributed computing infrastructure, while developing private and sovereign applications that operate with complete trust and compliance. Siloed collaborations thus disappear in favor of business actors and users controlling their data, decentralized identifiers and verifiable credentials. With an IND, an organization can now confidently prove the authenticity of its products, the integrity of its data and the identity of its employees.

1.3 Technological aspects: the union of decentralized identity and blockchain

Decentralized digital identity is a highly technology-driven concept due to its methods and interactions, which require several cryptographic layers to produce the expected functionalities. The value of combining decentralized identity standards with the various types of existing blockchain has been discussed in the scientific and IT literature since 2015[987] . On the IT side, IND does not always require the use of blockchain technology to maintain an online registry containing evidence of identity transactions. Centralized servers[988] may be more appropriate, for example when the incompatibility triangle studied in the first part[989] prevents a blockchain technology from meeting a company's needs for its use cases. Nevertheless, the advantages conferred by blockchain technology seem to be well known and particularly well suited to the DID and VC standards mobilized by IND. Indeed, to be inviolable and immutable, a verified attestation must be linked to a type of perennial register of verifiable data and evidence, i.e. to an open blockchain in the current state of the Web.

3.0. In 2023, there is not yet sufficient IT, legal and economic unanimity with regard to the many existing standards for the IND concept. This raises issues of interoperability between decentralized digital identity portfolios (PINDs) - studied below - which can then only communicate with a limited number of available verifiable proof registers (centralized servers versus open, decentralized blockchains). In this respect,

---

[986] The MINDS social network implements a decentralized identifier for each of its users on an optional basis, which means that this social network will be able to issue verifiable certificates in the future, "Minds raises $10M for decentralized and encrypted social network and messaging app", more information available at

[987] Report Ministry of the Interior, "Blockchain and digital identification - Restitution des ateliers du groupe de travail 'blockchain et identité' (BCID)", *op. cit.* 2020, version 1.0, available at.

[988] *Hardware Security Modules (HSM)* for maximum IT protection.

[989] See *supra*, I, Title 1, 2.3.2.

these 3.0 digital wallets may offer conflicting functionalities, and switching from one wallet to another may result in a loss of functionality for the user - situations that must be avoided if decentralized digital identity is to be massively adopted by Internet users. However, these difficulties are only partial, as essential functions such as storing verified credentials and receiving requests for proof are in principle supported natively and undifferentiatedly by all decentralized digital identity portfolios, thanks to its purpose-built 3.0 standards. An interactive map of some of these IND-related projects is available online, providing real-time insight into the projects under development for this new technological standard[990] .

1.3.1 The decentralized identity value chain

The notion of digital sovereignty is a fundamental component of distributed digital identity. To understand it, it is necessary to examine in the following sections the technical and legal aspects of its interoperability and modes of governance. These two pillars are essential to guarantee a secure and sustainable digital identity for Internet users. It is also important to understand how the new IT value chain offered by decentralized IND works. Some of its technical components are voluntarily not detailed in this study, due to their lesser relevance to other, more important issues recalled below. Decentralized identifiers (DIDs), verifiable credentials (VCs) and decentralized digital identity portfolios (PINDs) represent, for the purposes of this study, the three main fundamental digital pillars of this new 3.0 value chain.

1.3.1.1 Decentralized digital identifiers (DIDs)

Online identifiers are generally unique and temporary, used for specific contexts such as social networking platforms and online public services. Today, these digital identifiers are still under the administration of one or a few central authorities, which means they don't really belong to their users. Rather, in today's Web 2.0, they are granted and delegated free of charge by identity or online service providers, who subsequently remunerate themselves by collecting their users' personal data, usually in relative compliance with the RGPD. By offering an alternative to centralized digital identifiers (pair of IDs and passwords), IND aims to enable users to retain control over their decentralized identifiers (DIDs) without going through a supposedly trusted authority represented by an identity p r o v i d e r . Indeed, to represent their online identity(ies)

[990] To take part in the update or consult this interactive map, *go to* the following address

users need a unique digital identifier within the digital universe. Although there are many different digital identifiers for each person, such as e-mail addresses, social networking pseudonyms and telephone numbers, the IND introduces a new type of Decentralized Identifier (DID). This new type of identifier is unprecedented in that it uses cryptography to claim or prove a digital link in the form of a certificate or electronic signature, sometimes attached to a digital property. This DID standard was approved by the W3C in 2022 to become the second identification standard - after the now indispensable URL ("Uniform Resource Locator") - to be approved by this international institution. Decentralized identifiers cryptographically belong to users, as they represent unique digital links directly controlled by them. Multiple degrees of control and technological variants exist for this standard and for these DIDs, they systematically resort to cryptographic mechanisms well known since the 1990s, i.e. a pair of keys, one public and the other private, as previously explained. In this way, when the user is in possession of his private key, he alone owns and controls his identity attributes[991] . DIDs are considered decentralized by design, as each user is in principle able to control them individually, making them highly dispersed and portable on the Internet, enabling people to manifest their identity wherever they wish in the digital sphere. It's important to emphasize that the digital identifiers used in decentralized identity are not strictly "decentralized" in the IT sense of the term, but rather

The term "decentralized" is often used to describe these "distributed" identifiers, as they are most often attached to 3.0 trusted third parties, as this study suggests. Nevertheless, given that the term decentralized is commonly used in the context of DIDs, it is common to use it to describe these identifiers, even if this is not entirely accurate from a technical point of view. The use cases to which DIDs can be applied are almost infinite, and it's becoming possible to imagine a future in which DIDs are attached to all digital activities, including phygital ones: regal identity (CNIe), music playlists, videos, digital objects (NFT), blog posts, information, events, organizations, digital places (Metavers studied later). Search engines such as Google and Mozilla, as well as Apple, have formally disagreed, with a view to blocking adoption of the DID standard within the W3C standardization group, presumably because adoption of the standard would compromise their business models. During a vote in September 2021[992] , these three digital giants therefore voted against the adoption of the decentralized identifier standard, despite the fact that it has been under development by W3C and DIF since 2015. Although almost all the other members voted in favor of this standard, these

[991] Decentralized identifiers (DIDs) enable their cryptographic owner to present their identity to an online service, while proving that the information shared via this DID actually originates from them. This functionality is made possible by associating a public key with the DID, which can be communicated to third parties, while the private key is known only to the DID owner. The private key is then used to sign events or interactions linked to the same DID.

[992] DRUMMOND Reed, "Does the W3C still believe in Tim Berners-Lee's vision of decentralization", in *Eyernym*, October 12 2021, accessed online November 3 2021.

three players put forward four technical arguments to justify their vote, but these were quickly refuted by the entire working group. This attempt at contestation, which is in reality an attempt at oligopolistic destabilization with regard to this new high-potential IT standard, shows that the Web 2.0 giants are concerned about the possible regaining of control by Internet users relative to the growing trend towards decentralization of the Internet, which is gradually becoming 3.0. In this respect, it is worth noting that one of the pioneers and founders of the Internet, Tim Berners-Lee - a fervent advocate of decentralization - personally intervened to settle this dispute in favor of acceptance of the DID standard by the W3C and, by extension, for tomorrow's Internet[993] . Decentralized identifiers (DIDs) enable online interactions with other entities to be remembered, recognized and trusted. DIDs are created by a controller/issuer, which can be an individual, an organization or even software. The latter can use different authentication factors with a computing device, knowledge of a key or password, or body identity based on biometrics studied later[994] . In general, a combination of authentication factors is used to prove the legitimacy and authority of a decentralized identifier (DID). Unlike verifiable credentials (VCs), which are stored directly on the user's device or on a trusted server, DIDs can be stored in a verifiable data registry, such as a server or blockchain. In this way, any third party can verify the information and evidence published or sent by the entity behind a public DID. A private DID, on the other hand, is never stored on a public blockchain, and therefore cannot be accessed publicly. If a DID never contains personal data, it is suggested that a DID controller should be able to create several DIDs, to avoid re-identification by a third party. It is also recommended that temporary, single-use DIDs be created to comply with the provisions of the RGPD Regulation referred to above and the eIDAS Regulation, which is studied further on. On July 19, 2022[995] , the W3C finally announced that decentralized identifiers are becoming an official Internet standard. With 40 expressions of support at the time of its press release, this new next-generation standard became the most widely supported in W3C history. By way of comparison, the "HTML5" standard (which every Internet user uses on a daily basis) had only 19 expressions of support. This announcement confirms the theoretical interest of IND as a new standard for Web 2.0, and reinforces the interest of decentralized identity as the next foundation for Web 3.0[996] . According to Christopher

[993] "The director [of the dedicated W3C working group] concludes that the balance is in favor of the DID developer community, encouraging it to continue its work and seek consensus on standard DID methods. Objections [from Google, Apple and Mozilla] are rejected. The DID base specification is approved to proceed to W3C recommendation", Director's Decision on DID 1.0 Proposed recommendation formal objections, June 30, 2022, available at www.w3.org

[994] See *infra*, II, Title 2, 1.3

[995] "Decentralized identifiers (DIDs) v1.0 becomes a W3C recommendation", July 19, 2022, available at W3.Org

[996] Web 1.0 enables simple online data reading, *Web 2.0* enables online data reading and writing, and *Web 3*.0 enables online data reading, writing and ownership (the latter being a combination of *Web 1.0*'s original desire for decentralization and community governance with *Web 3.0*'s modern interaction features.

Allen, one of the promoters of the INAS concept - examined below - and co-author of the DID standard within the W3C, comments: "*DIDs are at the heart of our next generation of digital identity on the Internet. I'm delighted to see them recognized as an international standard. However, they are only the first step. To ensure a compassionate digital infrastructure that protects digital human rights, we need to design DID-centric architectures that exploit their decentralized capabilities and minimize the identities and credentials we share. We have laid an excellent foundation with the DID specification 1.0*"[997] . Finally, decentralized identifiers represent a breakthrough that makes the use of cryptography more accessible to the general public, by offering the possibility of controlling reliable, interoperable identifiers online. They also help to democratize the phenomenon of computer decentralization, enabling us to regain a form of control over the Internet, and perhaps one day over our digital avatars studied below[998] .

1.3.1.2 Verifiable digital certificates (VC) and verified certificates (VP)

Today, every citizen possesses certificates such as a passport to prove his or her identity abroad, a driver's license to attest to passing a national driving test, or a credit card to make purchases online or in stores. These physical certificates are thus used to confer and then attest to specific rights attached to each individual. However, sharing these certificates online is complex and sometimes risky, as there are few established IT standards to guarantee the reliability and interoperability of sharing such personal qualities and information. To address this issue, the verifiable credential (VC) data model offers a new mechanism for secure, verifiable expression of identity data online, while preserving confidentiality thanks to new cryptographic methods compatible with traditional IT infrastructures. These digital attestations can contain innumerable attributes such as images, permissions, consents, declarations or contractual obligations, to name just a few of their possible applications. A verifiable certificate enables its issuer to issue a set of verifiable claims to online services. More precisely, it is a digital file - standardized by the Decentralized Identity Foundation (DIF) - that contains declarations and proofs of information such as cryptographic keys, names, titles or qualifications concerning an entity (natural person, legal entity or connected object). As a reminder, a VC can be issued by one or more entities (such as

[997] W3C, "Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation. A new tool to empower everyone on the web with privacy-respecting online identity and consent-based data sharing", Press release, *op. cit.* at the following address
[998] See *infra*, II, Title 2, 1.4

issuers) and verified by any other entity (verifiers). A verifiable certificate is thus a tamper-proof credential whose author and content can be verified by cryptographic methods. According to a 2022 publication by Gartner on innovation cycles in digital identity technologies (*see* Appendix 9), verifiable credentials are currently in a "*trough of disillusionment*" phase, with a "*productivity plateau"* to be reached in 2 to 5 years' time. Instead, this research suggests that these 3.0 attestations are in a pre-industrialization phase, with some major social networking platforms such as LinkedIn beginning to offer - in partnership with Microsoft - this new digital standard since 2023[999] . Complementary to the DIDs mentioned above, these attestations have a high probability of being adopted as a new standard on the Internet. It seems important to make a semantic and IT clarification between a *Verifiable Presentation (VP*) and a *Verifiable Attestation.* Indeed, the former becomes the latter once its final recipient - the user - has received it and cryptographically signed it with his private key, using his decentralized digital identity wallet (PIND), which is discussed in the next section.

In EU law, the recent proposal to amend the European eIDAS Regulation ("eIDAS-2" studied below), favors a qualification and definition of verifiable (VC) and verified (VP) attestations as "*qualified attestations of electronic attributes*". This notion thus confuses VC and VP attestations, probably in favor of a quest for technological neutrality and a general scope specific to any EU Regulation (as mentioned for the MiCA Regulation and the proposed amendment to the TFR Regulation already mentioned). Across the Atlantic, California's state legislature has already introduced in a report dating from 2020[1000] , and then in a bill passed in 2022, the authorization for public institutions to issue in the form of legally recognized verifiable attestations of identification documents listed in section 1798.795(c) of the California Civil Code[1001] . In September 2022, a complementary law

---

[999] CHIK Joy, "LinkedIn and Microsoft Entra introduce a new way to verify your workplace", in *Microsoft Security Blog*.
"On LinkedIn, members will see an option to verify their workplace on their profile. With just a few clicks on their phone, members can obtain their digital employee card from their organization and choose to share it on LinkedIn. After submitting the credential, a location verification will appear on their profile.", free translation from English, available at the following address

[1000] "California blockchain working group". July 2020, p.32. Available at the following address:
"The California legislature should pass a law that allows public entities to issue, as authorized verifiable credentials, the identification documents referred to in California Civil Code section 1798.795(c) as verifiable credentials. Individuals would benefit from the ability to have these identification documents in a secure, verifiable digital form under their control. Verifiable credentials do not store any substantial personal information on the blockchain. Instead, decentralized identifiers (DIDs) would be stored to verify that the document has been validly issued and shared with the consent of the person concerned."

[1001] On February 17, 2022, Bill No. 1190 "Department of Technology: California Trust Framework" was introduced by Senator Hertzberg to require, by January 1, 2024, that the Department of Technology implement the "*California Trust Framework (CTF)*" to provide industry standards and best practices for the issuance of verifiable attestations to verify the information of a person or legal entity. The bill requires that the CTF be designed, to the extent possible, to be interoperable with other government trust and governance frameworks for verifiable attestations. Identification documents specifically include, but are not limited to, the following: (1) Driver's licenses or identification cards issued in accordance with Section 13000 of the Vehicle Code. (2) Identification cards of employees or legal entities.

relating to blockchain technology and aimed at amending section 103526.5 of the California Health and Safety Code[1002] has been adopted. This introduces the possibility of using IND and all types of blockchain technology to issue vital information such as birth, death and marriage certificates. This allows citizens to immediately prove their identity via QR codes or with enriched PDF files, rather than resorting to a postal mailing that takes several days, and is also more expensive than these new verifiable digital attestations. Finally, this qualification and legal recognition of VCs in California implies an unprecedented first qualification and legal recognition of this new conceptual and technological brick[1003] , which could inspire other legislation, notably in Europe (reference to eIDAS-2). This initiative would be a welcome step towards the regalian adoption of a more reliable, secure and emancipating IND for its users, and one that French legislators should draw inspiration from. As a reminder, VCs do not in principle store any personal information directly on a blockchain, but at most decentralized identifiers (DIDs), in order to verify that the document has been validly issued and shared by a public institution and with the consent of the person concerned. According to the CNIL, a verified attestation is never stored directly within a blockchain for reasons of limited computing capacity and risks of non-compliance with the RGPD. In the event of violation or loss of a verifiable attestation, the damage to its holder is limited, firstly because of the possibility for the holder to revoke it, and secondly because of a partial or temporary disclosure system limiting the risks of digital identity alteration (identity theft, forced revocation of attributes). In the future, VCs are likely to play an important role in helping individuals to achieve greater self-determination in a relationship of trust with accredited, more transparent organizations.

---

contractors. (3) Identification cards issued by educational institutions. (4) Health insurance or benefit cards. (5) Benefit cards issued under any government-supported assistance program. (6) Licenses, certificates, registrations or other means of exercising a business or profession regulated by the Business and Professions Code. (7) Library cards issued by any public library. California civil code, obligations : part 4 - obligations arising from particular transactions : title 1.80.a - Identification Documents : Section 1798.795. in *Justia Law*. Available at the following address, *see* also in *LegiScan*, available at the following address

[1002] Bill Text - SB-786, "County birth, death, and marriage records: blockchain," accessed September 30, 2022 at "Existing law requires that the certificate contain certain information and be printed on chemically sensitized security paper, as specified. This bill would authorize a county recorder to issue, upon request, a certified copy of a birth, death, or marriage certificate issued pursuant to these provisions, in addition to the required method described above, by means of a verifiable credential, as defined, using blockchain technology, defined as a decentralized data system, in which stored data is mathematically verifiable, that uses distributed ledgers or databases to store specialized data in the permanent order of recorded transactions."

[1003] *Op. cit.* note 1069, California SB1190, available at, "a cryptographically secure body of information, created in accordance with [W3C] open standards, that respects and protects all existing privacy protections and provides a portable, user-controlled means of sharing information in a manner that can be authenticated by publicly available services".

1.3.1.3 A decentralized digital identity wallet (PIND)

The rapid digitization of society over the past decade has been largely fueled by the advent of smart cell phones (smartphones)[1004] . In 2016, there were around 3.67 billion subscriptions to these ordiphones, a figure that has now doubled, and it is estimated that by 2026, 91% of the world's population will have access to a smartphone[1005] . On the strength of this now indispensable everyday medium for people's digital identity, IND standards could help solve the security problem raised by ANSSI in 2015, which stated that it was "*illusory to hope to achieve a high level of security with a smartphone*"[1006] . By 2022, according to European Internal Market Commissioner Thierry Breton[1007] , the introduction of a European Digital Identity Wallet (PIND) will enable EU citizens to store and use their data for a variety of services, such as checking in at an airport or renting a car. These wallets, available on cell phones or on the Web, will offer a secure and reliable identification service for citizens seeking both a high level of security and simplicity of administrative procedures linked to their civil identity. At this stage, we need to distinguish between (i) the current cell phone applications already available and provided by certain online services and major technology companies (GAFAM/BAHTX), (ii) third-generation mobile applications that implement the IND standards and mechanisms studied in this section. The former are referred to here as centralized digital identity portfolios, while the latter are referred to as decentralized digital identity portfolios (PINDs)[1008] . Indeed, while the functionalities of the former enable their users to perform certain actions relating to their identities (Apple Digital ID, federated digital identity already studied)[1009] , those of the latter use distinct and significantly innovative cryptographic functionalities. It is important to emphasize that decentralized identifiers (DIDs) and verifiable certificates (VCs) are structured and verifiable data, and not simply data shared in the form of PDF documents, as is common practice, for example, to certify identity information and online rights (CNIe, certificate of domiciliation). By receiving a multitude of these structured and verifiable DIDs and VCs directly via a PIND, it becomes possible for the first time to compartmentalize

[1004] According to the Commission d'enrichissement de la langue française, the term "smartphone" should be replaced by "smartphone". "multifunction mobile". This thesis, however, prefers the first term, to reflect the usual practices of the general public. Ministère de l'Education Nationale et de la Jeunesse, available at the following address
[1005] JP Morgan publication, "Payments are eating the world", [consulted online 28/10/2021], p.3.
[1006] ANSSI recommendation on security relating to ordiphones, July 28, 2015.
[1007] European Commission, "The Commission proposes a reliable and secure digital identity", [consulted online on November 10, 2021].
[1008] This term is introduced in this research, but has no official translation at present. Note that another possible name for these decentralized identity applications would be "*sovereign digital identity wallet - PINS*".
[1009] These mobile applications are centralized and their operations are not *open source*, meaning that their owners [GAFAM] refuse to share their computer code, which is protected and private, notably under cover of commercial secrecy. As a result, these players can resell certain personal data in a more or less opaque way, with the consent of their users. For more information, see "*Apple digital IDs come with conditions and costs*", on *BBC News*, accessed online on December 1, 2021.

identity information, enabling strict respect for users' privacy and personal data. A PIND is at the heart of any decentralized digital identity (IND) or self-sovereign digital identity (INAS) solution, as it enables the cryptographic mechanisms to work and articulate together. This local application runs directly on the user's mobile device, enabling him or her to establish relationships with third parties by setting up encrypted, P2P connections, i.e. without the involvement of multiple intermediaries often unknown to the user. Both parties to a transaction involving a PIND can thus use this encrypted communication channel to exchange verified information. The issuer of identity information can send a verifiable certificate (VC) in a matter of seconds to a user, who can then store it freely on his or her decentralized wallet, whose electronic signatures can be used to create a verified certificate (VP) that the user can choose whether or not to present to third parties, either to access online services and interactions, or in person (customs or police checks). Each user can thus verify the identity of the other party to establish a relationship of trust based on these proofs of identity 3.0, which are articulated by a PIND for the end user. In particular, end-users can keep track of the history of shared information, making it easier for them to exercise their right to data protection[1010] . Given that the PIND hosts several attributes and identity data, it is imperative to provide and guarantee data protection in the event of loss, theft or destruction of the user's device. The software functionalities of a PIND may vary according to the identity providers who develop them, but they often include a variety of hybrid systems using federated digital identity management (2.0) protocols.

PINDs are similar to crypto-asset wallets, in that they enable the sovereign ownership and management of cryptographic keys. However, the use cases and players in these markets are very different, and require a distinct approach in line with their specificities. In the medium term, it is likely that these two types of digital wallet will merge to ensure the reification of people's financial and administrative digital identities on the same mobile application. The European Commission has proposed certain standards to be implemented by suppliers for the standardization of a PIND (referred to as an "*EU Digital Identity Wallet - EDIW*")[1011] in accordance with the amendment to the eIDAS-2 Regulation mentioned below. In 2022, the Council of the EU has finalized its position on the introduction of a decentralized digital identity wallet with a high eIDAS guarantee level for EU member states. A transition period will allow the reuse of current digital identity solutions, such as Centric and Federated Digital Identity. Since 2021, the POTENTIAL

[1010] KOENIG Gaspard, "La propriété de soi", "En choisissant en amont, dans un smart wallet, quelles données j'accepte de partager et à quelles conditions, je pourrait réinstaller une forme de libre arbitre dans l'univers du nudge", accessed online November 18, 2021, p.10.
[1011] See *infra*, II, Title 1, 2.1.1.1.a, v. *op. cit.* "Blockchain and Digital ID Wallet: towards a decentralized European identity?", Ateliers Les Temps Numériques, EHESS, 2022, available at.

selected by the European Commission and made up of 19 member states, is coordinating six pilot use cases for the new European digital identity wallet prototype[1012] . This prototype and these use cases will be tested between 2024 and 2025, and new experiments will be implemented from April 2025[1013] . At the same time, the NOBID consortium[1014] , which includes Germany, Italy and a number of Northern European countries, is working on the development of a European digital identity wallet to enable banking and financial interoperability. As far as liability is concerned, it would appear that PIND providers are not systematically liable for the data they transmit. In the event of loss, theft or identity theft, while in principle the responsibility for data verification should lie with the system provider, the PIND manufacturer or the data provider who has provisioned VCs on the PIND, the user may also - in certain cases - assume part of this responsibility if negligence or fault on his part is reported (in the case of careless exposure of his data). While blockchain technologies natively enable time-stamping and cryptographic signatures that are useful for users, notably for proving the possession of funds or for voting, there are new, more sophisticated cryptographic mechanisms for proving information with certainty without revealing any information beforehand. Finally, according to Gartner's July 2022 publication of its innovation cycle chart for digital identity technologies, the PIND concept has reached the "*peak of its attractiveness*"[1015] , a partly surprising perception given the state of this market segment, which is rather in the pre-industrialization phase in view of the adoption of the eIDAS-2 trust framework. Pragmatically speaking, Gartner estimates that a "*productivity plateau*" will be reached within five to ten years for this technology brick.

1.3.1.4 Backup, recovery and responsibility for decentralized identity attributes

When a person has the power to control and manage their data, it's their responsibility to protect and control it to avoid accidental loss, such as the loss of their computing device or cryptographic keys when they store it. As with any other identity medium, a reliable backup mechanism is needed to restore accumulated or lost data should the need arise. If such a backup mechanism is not available, the user may not be able to restore all or part of the attributes accessible via his PIND. Visit

[1012] The use cases included in this consortium are: (i) bank account opening, (ii) electronic driving license attestation, (iii) online public service(s), (iv) electronic signature, (v) electronic prescription or (vi) electronic SIM card registration. "POTENTIAL Consortium: towards a European digital identity portfolio", consulted on December 20, 2022. For further information, visit the website at the following address
[1013] *Ibid*. POTENTIAL Consortium.
[1014] NOBID Consortium, December 14, 2022, for more information visit
[1015] V. Appendix 9.

In practice, given that decentralized digital identities will probably be linked at source to trusted 2.0 third parties (CNI, passports), it is likely that the mechanisms for safeguarding and recovering the 3.0 attributes generated will again involve these same players, i.e. a form of recentralization by the same institutions and public services we have already mentioned (FranceConnect, etc.). There are therefore several options for safeguarding decentralized identity attributes (DID, VC), depending on the requirements, procedures and governance specific to each use case. Basically, backup can take the form of an encrypted file[1016] containing the cryptographic keys[1017] and other associated information directly saved and retained by the user. This implies that the user stores the file in a secure container that is more or less intuitive to access and specifically developed by identity providers, and then saves, for example, his unique and personal recovery phrase (private key). However, this also implies a high level of responsibility on the part of the user, who must have sufficient knowledge to master and store his or her cryptographic keys. In other words, this encrypted file can be stored locally on the user's device, in the case of an INAS self-sovereign identity, studied in the next paragraph, or downloaded from an external server, admittedly IT centralized, but legally guaranteed because hosted by a certified trusted third party such as a "*sovereign cloud*"[1018] . This second mixed option consists of using a mechanism for splitting the private key into several parts, which the user can then send to various trusted contacts (family members, notaries, lawyers). This procedure would be easy to execute via a PIND, but may not be viable for people who do not have access to multiple devices or who are isolated. A third and final option is to back up data with a trusted third party, who alone will guarantee the backup and enable data recovery for the end-user in the event of loss of access. In 2022, there is still no unanimity regarding these authentication methods and how to avoid abuse by so-called trusted third parties 3.0, supposedly more reliable than with the use of 2.0 tools. In the short term, it is likely that this third option will be the one most used by identity providers for their first implementations of decentralized identity portfolios, notably to ensure a simpler and more intuitive user experience than the first option, which is certainly more liberating for Internet users, but more complex and therefore utopian. In principle, each provider of a decentralized identity solution should offer several options

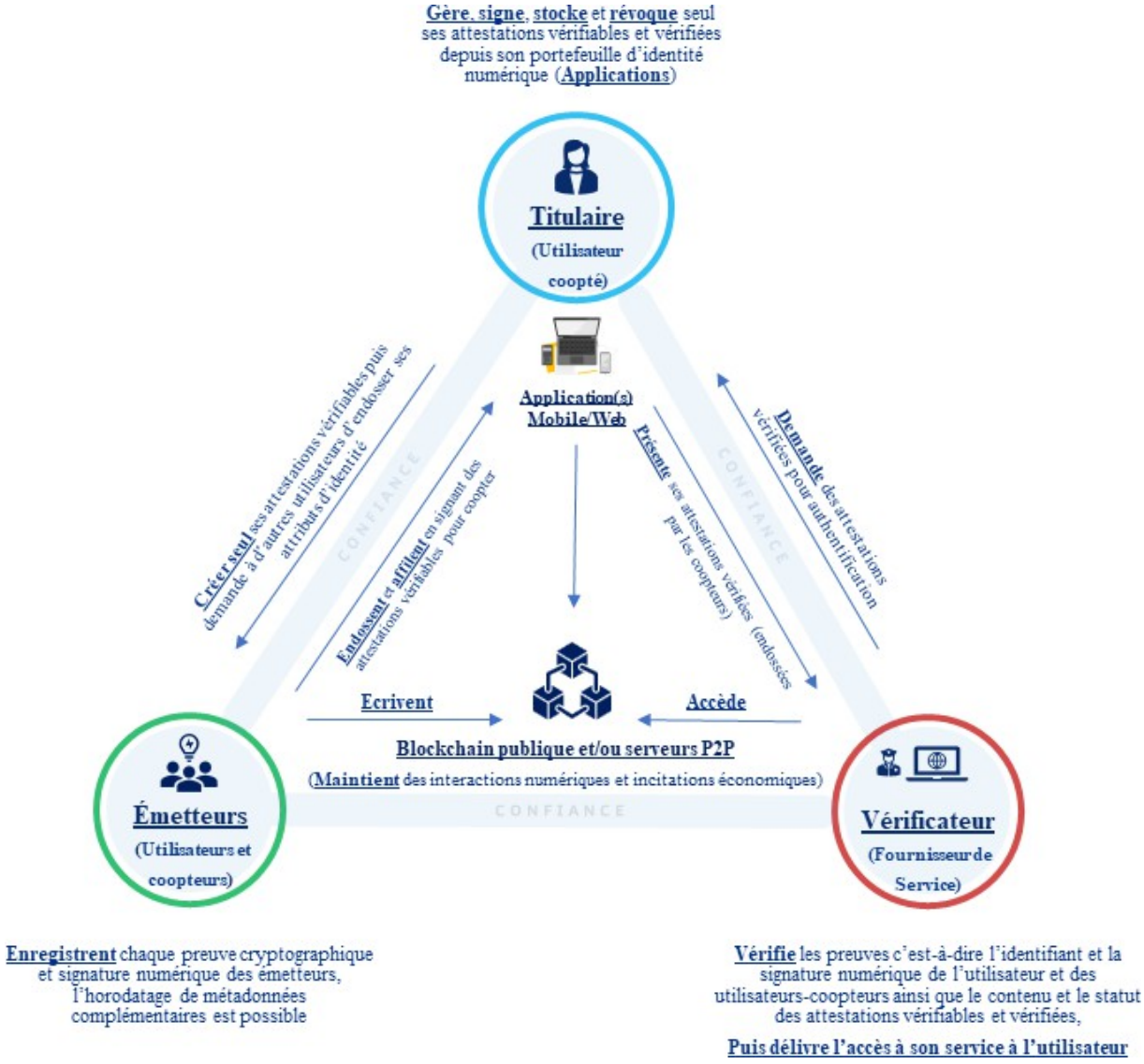
[1016] The term "decipher" is preferred to "decrypt", which is often used incorrectly. For further information, please consult the following link

[1017] For a key to be restorable and readable by a human being, it is given in the form of a sentence (also known as a "*recovery phrase*" or "*mnemonic seed"*) generally made up of 12 or 24 words. This mechanism has been used for over a decade by crypto-asset wallets. For more information on crypto-asset wallets, see the following link. To understand the random and 'private' nature of a *private key,* see the following link

[1018] Reference is made to the European "Gaia-x" initiative, as well as to the standard and list of *qualified cloud computing service providers* issued and updated by ANSSI. In theory, these *keys* are indispensable for successfully restoring the data attached to a decentralized digital identity portfolio. In practice, however, the risks of loss or theft of these identifiers are numerous and difficult to avoid for the general public. As a result, identity providers will most likely reserve the right to retain these keys in one way or another, in order to provide a backup in case of need.

and as intuitive as possible for users. It should be remembered that identity providers will have to comply with the new rules of the eIDAS-2 amendment, studied below, in particular by integrating a secure element, i.e. a physical security component built into the user's mobile device, necessarily linked to his PIND and IT device (cell phone). This material requirement imposed on identity providers, to the benefit of more secure storage of users' cryptographic keys, could significantly delay the adoption of European IND solutions. Finally, responsibility for the management and accuracy of these 3.0 attributes (VC, DID) rests with the various parties involved in the decentralized identity attribution and verification chain. In the semi-centralized versions that this study suggests will be most common in the short and medium term for third-generation, IT-distributed digital identity, identity providers are responsible for verifying the accuracy of the information provided by each user, ensuring that attributes are relevant to previously targeted contexts of use. Finally, in a highly decentralized version (the case of INAS), identity attribute holders are responsible for updating their attributes in a timely manner, ensuring that they are accurate and that their storage is perennial. Attribute recipients are also responsible for verifying the accuracy of attributes before using them for any action or decision related to a digital identity. Transparency and collaboration between the parties to an IND, as set out below, seem essential today to ensure that decentralized identity attributes are reliable, accurate and relevant to each context of use.

1.4 Self-sovereign digital identity (INAS) at the height of decentralized identity



Self-sovereign Digital Identity (SDI) is based on the fundamental principle that each individual should be solely responsible for issuing and managing his or her own digital identity, without being dependent on a third party. In this third-generation model of the digital identity concept we have studied, decentralization is taken to the extreme, with the aim of achieving IT and social autonomy in digital identification and authentication, as illustrated above by the INAS-specific triangle of trust. Here, users are able to issue and manage their verifiable credentials and identifiers autonomously and independently.

decentralized[1019] . INAS enables individuals to privatize their digital identities at their own discretion, whether informatically, socially or even economically, without requesting any authority to issue a digital identity attribute, unlike the distributed digital identity (IND) model[1020] illustrated by the - relatively similar - diagram studied earlier. In 2020, specialist and Professor of Law Ignacio Alamillo Domingo proposes a fairly precise definition of the INAS:

"The adoption of ISS principles implies (...) *increased complexity in trust management and a shift from hierarchical or federated trust guarantee frameworks (...) towards socio-reputational trust models based on consensual guarantee frameworks, notably through the use of quantifiable methods for aggregating trust in digital claims and identities*"[1021] . This significant cryptographic personalization thus seems to serve users and web surfers by promoting the online exercise of some of their fundamental rights (such as art. 10 and 11 of the DDHC)[1022] . Assuming that a majority of Internet users and citizens learn to use a pair of public and private cryptographic keys, the self-sovereign digital identity would, by design, present certain IT and legal advantages for its users, such as consent, pseudo-anonymity, interoperability, ownership and cryptographic portability of their personal data. If self-sovereign identity (INAS) is to distributed identity (IND) what Bitcoin is to blockchain, i.e. a highly decentralized and socially disruptive first application, then INAS is likely to face similar social, technical, legal and political challenges and reactions. Because it opens the door to a new identity ecosystem independent of direct government oversight and approval, it is likely that the concept of distributed, semi-centralized and hybrid digital identity will become more widely adopted in the medium term than this notion of INAS entirely under the cryptographic control of individuals. However, while INAS supports the idea o f a universally accepted digital identity

---

[1019] Semantically, there are several possible translations from English "*Self Sovereign Identity*" into French. In early 2023, the French translation of the proposed amendment to the eIDAS Regulation ("eIDAS-2") proposed a first legal translation in its recital (34) with the term "*autonomous identity solutions*". This thesis favors the term "*self-sovereign digital identity*" and its French acronym "INAS" over its English equivalent "Self- Sovereign Identity - SSI". Indeed, the acronym "SSI" is commonly used in the IT industry to designate the
As the French acronym for "Sécurité des Systèmes d'Informations - SSI", it can hardly be reused as an acronym. A similar observation applies to the French acronym "IAS", already used by the Agence Nationale des Titres Sécurisés (ANTS) to designate "Identification, Authentication and Signature - IAS". The use of the latter acronyms could thus be a source of confusion with regard to this concept of self-sovereign digital identity. v. also "Proposition d'une taxonomie francophone pour l'identité décentralisée", 2021, ⟨hal-03398096⟩.

[1020] The term *distributed digital identity (IND) is used* in this and the following sections to refer to *decentralized digital identity (IND)*. This is the same concept, and the acronym "*IND"* can refer to this concept without distinction. This change of term is nevertheless intended to avoid a misunderstanding in this section concerning the fact that a decentralized digital identity is not in fact completely "*decentralized*" in computing terms, but rather "*distributed"* in relation to an INAS, which is assumed to be completely decentralized, as mentioned in this section.

[1021] Dr. ALAMILLO DOMINGO Ignacio, "SSI eIDAS Legal Report", for European Commission, accessed online 06/08/2021, p. 26.

[1022] Art. 10 of the Declaration of the Rights of Man and of the Citizen of 1789: "No one shall be troubled for his opinions, even religious, provided that their manifestation does not disturb the public order established by law", and *v.* Art. 11: "The free communication of thoughts and opinions is one of man's most precious rights: every citizen may therefore speak, write and print freely, subject to liability for the abuse of this freedom in cases determined by law".

accessible without a trusted third party, it seems important not to exacerbate or erase the cultural diversity that already exists by paving the way for countless singularities and affiliations to be claimed online. As German sociologist Andreas Reckwitz points out, "*singularization can lead to new forms of inequality between those who assert themselves in a world of singularities and those who are unable to do so for lack of means*"[1023] . Could this social desire for singularization of our online selves lead to the emergence of a libertarian INAS culture similar to that existing in the world of crypto-assets? This would seem plausible, given the proximity of these two spheres in both social and IT terms, and their inevitable convergence. However, if INAS can contribute to a form of liberation of people's identity online, it must be ensured that it does not exacerbate social, cultural and economic inequalities, i.e. that it respects positive law so as not to encroach on the rights of others, notably under the guise of anonymity. This paradox therefore needs to be emphasized and taken into account when designing and interacting between IND and INAS solutions, both by private identity providers and by state services. In the longer term, it is assumed that self-discovered digital identities will become established in digital environments that were initially assumed to be unregulated, such as Metavers[1024] , the crypto-asset market or certain peer-to-peer exchange systems (*see* Decentralized Finance, DAO, tbDEX[1025]). These concepts and technological bricks can be merged or even fused with self-discovered identities to form new online use cases. INAS also offers a solution for creating decentralized universal proofs of existence. However, this represents both an IT and societal challenge for traditional trusted third parties in the digital identity sector, and a social and legal opportunity for the digital freedom of Internet users. Although the design of such a decentralized digital humanity is now possible thanks to 3.0 solutions such as the Proof of Humanity (PoH) project already mentioned, a balance between digital freedoms and social stability needs to be found and discussed. It is crucial not to fall into the illusion of total control by individuals, ultimately subject to the digital control of oligopolistic entities similar to those already active in Web 2.0 and gradually infiltrating Web 3.0. It's important to remember that the Internet was supposed to liberate people philosophically, not lock them up.

In terms of liability, a distributed digital identity solution (IND)[1026] does not have the same legal effects as a self-sovereign digital identity solution (INAS). The diagram

---

[1023] RECKWITZ Andreas, "Singularization has become a mass phenomenon", 2022, in *Libération*, researcher attached to the Georg Simmel Centre (EHESS/CNRS), available at

[1024] BASDEVENT Adrien, FRANCOIS Camille, RONFARD Rémi, "Mission exploratoire des Métavers", 2022, available on vie-publique.fr

[1025] See *infra,* II, Title 2, 2.3

[1026] *Op. Cit.* The term *distributed digital identity* (IND) refers to and echoes that of *decentralized digital identity. It is* the same concept, and the acronym "*IND"* can refer to this concept without distinction. This change of term is nonetheless intended to avoid a misunderstanding in this section concerning the fact that a decentralized digital identity is not in fact completely "*decentralized*" in computing terms, but rather "*distributed*" in relation to an INAS, which is completely decentralized as mentioned.

presented above differs from the above scheme in that DIDs and VCs are not validated by centralized or distributed servers managed by state or private entities. Instead, they are verified directly between users and an open blockchain such as Bitcoin[1027] or Ethereum[1028] . In an INAS system, no public or private entity is legally responsible for the proper functioning of identification, authentication and authorization of access to digital services by users. In theory, therefore, users have exclusive responsibility for reasonably managing their digital identifiers (DID, VC) and their PIND (including cryptographic keys), as if they were managing crypto-assets, i.e. without recourse to multiple trusted third parties. However, it is illusory to think that a digital identity, particularly a social one, can exist without the involvement of a recognized proxy, whether a public or private authority. Indeed, in the event of a dispute involving exclusively self-sovereign identities, a holder could find it difficult to prove the failure of his or her INAS system, which is decentralized from end to end and does not rely on any trusted third party. In such cases, a judge might consider that an IND solution with a trusted third party would have been more reliable, and therefore place responsibility on the conflicted digital identity holder, as he or she had exclusive control over it. The developers or players in public blockchains or IND solutions could hardly be held liable in this specific case. In marginal reality, however, this situation could not apply to all citizens due to their often unequal IT skills, in reference to the growing "*digital divide*"[1029] . To be successful, self-sovereign digital identity would require, in the short and medium term, the necessary acceptance by governments and institutions, which tend to reject the most decentralized technologies in terms of IT and social issues. In this respect, it is possible that a form of distrust between INAS and IND attributes will manifest itself on digital identity markets. This means that hybrid digital identity providers
2.0 and 3.0 could create 'predicates' or 'restrictions' on other attributes derived from INAS, which must demonstrate its technical, legal and political soundness, for people and their future digital behaviors. Today, it's still early days for an international IT implementation of INAS, but there are many promising and rapid developments within the most decentralized Web 3.0 communities. Nevertheless, it does seem that a proliferation of self-sovereign identity solutions is dependent on an understanding and legal recognition of some of its computational components, as the history of the evolution of the Internet studied earlier in this thesis seems to demonstrate.

[1027] V. Appendix 3, Focus 1 to 6.
[1028] V. Appendix 6, Focus 2. See also *infra,* II, Title 2, 2.1
[1029] BEN YOUSSED Adel, "Les quatre dimensions de la fracture numérique", in *Réseaux*, 2004, available online

1.5 Factors and limits to the adoption of decentralized digital identity

In recent years, significant progress has been made in the field of decentralized identity by governments, companies and institutions such as W3C and DIF, thanks to pilot projects that have used distributed/decentralized digital identity standards and (mainly closed) blockchain technologies. The technological and social benefits of using an IND are gradually coming to the fore. The recent proposal to amend the eIDAS Regulation suggests that decentralized identity can significantly reduce the costs associated with verifying an identity, regardless of the level of guarantee and trust required by this Regulation (low, substantial or high level). For example, a person can carry out an online verification of their official identity documents just once, and then receive associated verifiable and verified attestations (VC and VP), which they can then use for several online services without needing to re-identify each time. Decentralized identity mechanisms also enable compliance with RGPD requirements, further reducing the costs associated with data privacy compliance. However, the adoption of the mentioned decentralized digital identity standards (VC, VP, DID, PIND) is still far from reaching its IT potential. This is due to difficulties in finding a reliable and sustainable business model for identity and service providers. When a new technology emerges, the search for IT and social disruption takes precedence in the short term over the search for economic profitability or legal compliance. IND's current solutions are not yet satisfactory for consumers and businesses alike, and their benefits vary significantly according to their market segments. The search for non-intrusive and transparent business models, by decentralized identity providers, also seems to be a fundamental element in the short and long term to ensure the success of this promising ecosystem.

The concept of decentralized digital identity faces several structural obstacles. Firstly, there are computational challenges linked to the complexity of 3.0 cryptographic mechanisms. Secondly, legal issues such as the qualification, recognition and legal harmonization of INDs, including blockchains, must be taken into account for the future of this Web 3.0 in which it is embedded. There are also political issues at stake, if only because the term "decentralized" is still often wrongly associated with crypto-assets in France, demonstrating the need and importance of educating the legislative and executive bodies. Finally, there are the experiential issues, i.e. the simplicity of managing a digital identity offered by verifiable and verified credentials (VC/VP), which must not lead to an overloaded or unintuitive experience of accessing online services. Users must also make reasonable use of their VC/VP online to avoid excessive use of their identity attributes. To guarantee a reliable and privacy-friendly decentralized identity, it is necessary to design solutions that respect confidentiality and security standards throughout their life cycle.

life cycle and under the concept of "*programmed confidentiality*" initially introduced by the CNIL[1030] . It is also crucial to identify and limit malicious actors who could offer decentralized identity portfolios for deceptive or illegal purposes. Decentralizing user information is another important security measure to minimize the risk of hacking. In addition, it is important to associate strict standards with these solutions to guarantee respect for online rights. According to Everett Rogers' theory of the diffusion of innovation[1031] , the diffusion of a new technology depends on five characteristics. It is argued that decentralized digital identity already partially meets these five criteria: (i) relative advantage, (ii) compatibility, (iii) complexity, (iv) demonstrability and (v) observability. What's more, Lindy's law[1032] seems relevant to decentralized digital identity, meaning that the more the IND is used over time, the longer its lifespan and the lower its failure rate. Ultimately, it seems that decentralized identity will eventually take hold, but the question is where, when and at what pace.

1.5.1 Computer science and open knowledge at the heart of IDN

1.5.1.1 The importance of free software and open source codes

As a foreword, it is important to make a distinction between the notion of transparency mentioned throughout this study, and that of explicability[1033] for 2.0 and especially 3.0 computer programs. Transparency presupposes that computer code is open and public, and can therefore be examined by numerous peers around the world (developers, researchers). Explainability, on the other hand, refers to the comprehensibility and intelligibility of the functioning, interactions and purposes of a computer program. Ideally, these two notions should be combined to ensure maximum digital confidence for all players involved in 3.0 technologies (suppliers, users, legislators). Originally,[1034] software was more or less free depending on the wishes of its creators, the very nature of the software enabling its distribution.

[1030] The decree published on August 31, 2019 in the Journal Officiel offers new French equivalents for the English-language term of the "privacy by design", now translated as "programmed confidentiality", "Vocabulaire du droit (liste de termes, expressions et définitions adoptés)", JORF n°0202 Texte n° 91, resource available at the following address

[1031] BENOIT-GUILBOT Odile, "Rogers Everett M., Diffusion of innovations", 1964, *Rev. Fr. Sociol.* 5, in Persée, 1964, accessed August 5, 2021, p.15, available online

[1032] ELIAZAR Iddo, "Physica A: Statistical Mechanics and Its Applications", 2017, vol. 486, issue C, 797-805. *Lindy's Law* states that the longer a non-perishable concept, such as a perennial technology or idea, has survived and is still in use, the more likely it is to have a long life. *The Lindy effect* shows that, when this law applies, the failure rate of a technology decreases over time. According to this theory, decentralized identity has not yet reached its critical threshold, unlike some public blockchains such as Bitcoin and perhaps Ethereum. However, our study suggests that decentralized identity will benefit from this law once it has been massively adopted (which takes time).

[1033] *Op. cit,* JEAN Aurélie, "Les algorithmes font-ils la loi?", reading position in the book: 61%.

[1034] BRAUDO Serge, "Logiciel - Définition", in *Dictionnaire Juridique*, "Un 'logiciel' est, selon le vocabulaire officiel de l'informatique, 'l'ensemble des programmes, procédés et règles, et éventuellement de la documentation, relatifs au fonctionnement d'un ensemble de traitement de données' (JORF 17/01/1982)", available at the following address

and its modification[1035] . However, when software suppliers began to differentiate themselves from hardware suppliers, contractual licenses[1036] were introduced to govern the conditions of software use, such as access rights to source code or modification rights. The concept of "free *software*" has been gaining in importance since the 2000s, and is now considered by specialists to be a "(...) *mixture of product (finished object) and service (managing the adaptation and evolution of this object). It is precisely this duality that is the origin and interest of free software*"[1037] . Richard Stallman, an American MIT researcher and programmer, is considered the founder of the free software concept. In 1985, he defined four essential freedoms associated with free software and created the "*Free Software Foundation*"[1038] to defend these freedoms by granting specific software licenses. Firstly, the freedom to run the software without limitation of use, purpose or territoriality. Secondly, the freedom to study the functioning of the software, to obtain source codes, to modify or adapt them to specific needs. Thirdly, the freedom to redistribute the software to any third party, free of charge or for a fee, without restriction. And fourthly, the freedom to publish and distribute modifications made to an original program. To guarantee these freedoms, access to the source code of free software is an essential condition, and the software must be available in the form of editable sources. The principle of free software offers users the freedom to run, copy, distribute, study, modify and improve the software. This freedom enables users to control the program and adapt it to their needs, individually and collectively. A parallel can be drawn under French law with "*free software*" licenses, in which case the author of the computer program cannot prohibit the writing of a new program with similar functionalities, compatible and interoperable with the computer standards of the initial program. Free software is protected by copyright and the provisions of the French Intellectual Property Code. These licenses allow users to copy, modify and distribute the software freely, but require that all modified versions are also free. These licenses are widespread[1039] and the most protective to date. In this way, a greater number of people can contribute to open source code(s), fostering innovation and the security of IT infrastructures and online services. In Web 3.0, and more generally in the world of IT, open source is the key to success.

[1035] VALERIAN François, COMBY Gérard, KAPPELMANN Alexia, GIMON Magali, et al. " Annales des mines n°18 sur les enjeux numériques : Propriété et gouvernance du numérique ", quarterly series - N°18 - June 2022, Institut Mines-Télécom,
"[...] the free software approach does not represent a denial of intellectual property, but a new way of managing it.", available at the following address, p. 71.

[1036] A software license is a contract covering the rights and obligations of users, by which the owner of copyright in a computer program defines with its co-contractor (operator and/or user) the conditions under which this program may be used, distributed or modified.

[1037] *Op. cit.* "Annales des mines n°18 sur les enjeux numériques: Propriété et gouvernance du numérique", p.72.

[1038] Free Software Foundation, "For more than 20 years, FSF's Licensing and Compliance team has been the leading resource on open source licensing for open source developers," see the website at

[1039] For more information, visit Choose a License - *choosealicence.com* and see also Browse Licenses - *tldrlegal.com*

he terms "*free software*" and "*open source"* are regularly used interchangeably, although they convey realities that it seems important to distinguish in computing. According to Richard Stallman, there is a notable distinction: "*The terms 'free software' and 'open source' cover roughly the same range of software. However, they say profoundly different things about that software, because they are based on different values. The free software movement campaigns for the freedom of computer users; it's a movement that fights for freedom and justice. The open source ideology, on the other hand, focuses mainly on practical benefits and does not campaign for principles*"[1040] . In fact, most open source software is free software. Open source software is therefore often free software, i.e. open, but it is not necessarily accessible free of charge, unlike free software, which is free by design. A crucial aspect of free software is that users are free to cooperate. It is absolutely essential to allow users who wish to help each other to share their patches and improvements with others. By attracting a growing number of people around a collective, open project, free software represents a formidable means of sharing decentralized skills and knowledge on a social level. Moreover, in 2009, the pseudonym behind the creation of Bitcoin[1041] , Satoshi Nakamoto, explained his vision of the open source nature of his innovation in these terms: "*Being open source means that anyone can independently examine the code. If it was closed code, no one could check the security. I think it's essential for a program of this nature to be open source*"[1042] . In this respect, while the foundations of the Internet advocated maximum transparency, i.e. open source for the computer programs that make it up, today it turns out to be made up more of proprietary (closed) than free (open) software. Thus, the Internet has progressively lost the battle of free software to proprietary software, but it is suggested that blockchain technologies may, for the first time, be able to offset this trend, thanks to the free and open source software of which they are composed. In this respect, it is emphasized that fighting against IT decentralization, as studied above, indirectly amounts to fighting against an Internet based on more free software (3.0). This is because public blockchains are based on and promote the open, accessible nature of software and protocols[1043] . Conversely, hybrid and private blockchains are based on software that is initially free, but gradually becomes proprietary. As mentioned above, it can be misleading to think that the notion of free software is synonymous with free, although some of the free software we use remains free, such as VLC media player[1044] and Firefox[1045] . In reality, being free is just a side-effect of being free.

[1040] STALLMAN Richard, "How open source loses sight of free software ethics", in gnu.org, accessed online on October 27, 2021.
[1041] V. Appendix 3 and Appendix 6, Focus 1.
[1042] NAKAMOTO Satoshi, "Re: Questions about Bitcoin", 2009, in *satoshi.nakamotoinstitute.org*, available at
[1043] In other words, public blockchains and their degree of pure decentralization are merely a new form of tool in the service of a free software victory.
[1044] VLC Official site - Free multimedia solutions for all OS - VideoLAN. Available at the following address
[1045] For more information, see the list of free and open-source software at the following address

the license under which the authors chose to distribute them at the time of their creation. Finally, the importance of the open nature of software seems to fit perfectly with the concept of decentralized computing in 3.0 technologies. Together, these two concepts form a kind of counterweight to the openness and transparency of the Web, an orientation that should at the very least be preserved or reinforced.

1.5.1.2 The importance of joint IT and legal education

If the "*HyperText Transfer Protocol - http*" standard had not been open and free when it was created and developed in the early days of the Web, the Internet would probably never have seen the light of day in its current form (its adoption would not have been exponential). It is suggested that this observation also applies to decentralized digital identity standards (VC, VP, DID). This leads this research to the importance not only of the aforementioned openness of these IT standards, but also of the education and knowledge required for their dissemination and adoption. For example, while the majority of the general public is not familiar with the details of the "*http"* protocol, most seem to know the more intuitive principle of the "*green padlock" at the* top left of the browser, which attests to relatively secure online browsing. For decentralized digital identity, a similar standardized and intuitive mechanism could be put in place to make it easier for users to understand the advantages and conditions of using an IND, like the "*cyber score*" principle already mentioned[1046] or the "*EU trust label for digital identity portfolios*" studied previously[1047] . In theory, to make informed decisions, individuals need to be informed, and a wealth of knowledge is essential to understand the benefits of using an IND. However, as Jean-Jacques Quisquater pointed out at a conference in 2021[1048] , there is a shortage of manpower in this sector, as there is a lack of IT specialists with sufficient knowledge of blockchain technologies and IT security specific to the Semantic Web (3.0). To meet this challenge, educational resources need to be available in different languages and formats (videos, infographics, text, media, audio), and on different platforms (books, articles, social media, TV) tailored to the target audience (children, businesses, lawyers, government representatives, senior citizens)[1049] . Decentralized identity providers, educational establishments, public authorities

[1046] See *supra*, I, Title 1, 2.3.1.1.
[1047] See *supra*, II, Title 1, 1.3.1.3.
[1048] The following remarks collected from Jean-Jacques Quisquater at the International Forum on Cybersecurity (FIC), 09/09/2021, Round Table: "What alternative models for identity?", "There aren't enough computer scientists who know enough about blockchain technology and IT security".
[1049] DOUTAUT Vincent (Dir.). "Informatique et culture scientifique du numérique", pp.1-433, 2021, "It is [...] crucial that the new generations, high school and college students alike, get to grips with these issues and are introduced to them through the education they receive. Over and above the services provided by digital technology, it is vital that people understand the legal, political and ethical implications", available at the following address

must ensure that these educational resources are available and, above all, up to date. The future European blockchain (EBSI) is already providing online educational resources for the public, both at national and EU level, as mentioned in part one[1050] . To reach the critical threshold of knowledge, it is necessary to convince civil society of the advantages of this technology: trust, confidentiality, partially decentralized storage and asynchronous verifiability of evidence and identity attributes. It is also important that distributed identity systems are designed so that as many players as possible can participate in understanding them, which is already a challenge for traditional (2.0) digital identity systems, but even more so for decentralized ones. To guarantee inclusiveness, we also need to develop barrier-free access for people affected by the digital divide, who are already disadvantaged by the use of these new digital tools. For example, people who do not have the legal capacity to act can still use an IND by relying on a trusted third party, called a guardian[1051] , thanks to a cryptographic key delegation system currently being developed and standardized by the W3C. Finally, the difficulties of IT law lie in the lack of information available to the general public, while IT professionals are aware of the many possibilities and impossibilities (myths) of IT. In view of this, education about the IND must be accessible to all Internet users, and not just to IT specialists who might hijack certain mechanisms and uses for ideological, political or commercial ends.

Chapter 2: Towards perfect, augmented cryptographic law

2.1 Regulatory compliance in Europe: identity providers and trust services

2.1.1 Centralized and decentralized digital identity framework (eIDAS-1 & 2)

2.1.1.1 The eIDAS Regulation

Many legal experts believe that today's digital identity is already regulated by principles relating to personal data, privacy protection and electronic identification and authentication[1052] . Since July 23, 2014, the eIDAS Regulation No. 910/2014/EU, here referred to as "eIDAS-1", provides a precise definition of electronic identification as a

"the *process of using personal identification data in electronic form*

[1050] European Blockchain Service Infrastructure (EBSI). [Video]. YouTube, resources available at

[1051] Art. 1242 of the Civil Code, in the version in force since October 1er 2016, states "One is responsible (...) for the things one has in one's custody". In the context of a decentralized digital identity, a person who does not possess the technical skills to manage his cryptographic keys himself, could delegate this task to a trusted third-party manager, who will act as the "*custodian*" of his keys. In this way, delegating cryptographic keys to a third-party manager facilitates access to a decentralized digital identity for people who do not possess the necessary IT skills, while guaranteeing the security and confidentiality of their data.

[1052] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, *op. cit.* "L'identité numérique; quelle définition pour quelle protection?", 2020.

univocally representing a natural or legal person, or a natural person representing a legal person"[1053] . Authentication is also defined as "*an electronic process that confirms the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form*"[1054] . The preceding definitions do not seek to define identity as such, but rather to provide a definition that addresses the intangible elements of identity without describing it precisely. These definitions focus on the identity of natural and legal persons, without encompassing that of machines (servers, computers)[1055] . The first version of this Regulation was negotiated between 2013 and 2014, published on August 28, 2014, and came into force on September 17, 2014. Partial implementation of the Regulation began in July 2016 for the first trust services[1056] , followed by full implementation in September 2018 for national electronic identification schemes and means[1057] . The aim of eIDAS-1 was to create an interoperable environment for the various digital systems set up within member states for the purpose of fostering the development of a European digital trust market. It is based on various amendments to existing legislation, such as the May 20, 2015 Directive on the prevention of the use of the financial system for the purpose of money laundering[1058] and the November 25, 2015 Directive on payment services in the internal market[1059] . The Regulation also lays several foundations. On the one hand, it establishes common and mutual IT communication standards ("*eIDAS nodes*")[1060] enabling the reliability of digital services certified as trustworthy to be assessed[1061] , and on the other, it institutes a common pillar for digital identification services for European citizens. In the sense of this Regulation, digital identification is a digitally verified and authenticated identification, whose level of guarantee is considered high for its users. Visit

[1053] Art. 3.1 of Regulation (EU) No. 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L, 2014, accessed September 15, 2021.
[1054] *Ibid*.
[1055] See *infra*, II, Title 2, 1.6
[1056] In 2016, eIDAS distinguishes five trust services (each with two or three underlying *levels of trust*): (i) *electronic signatures* for natural persons, (ii) *electronic seals* for legal entities,
(iii) *electronic time-stamping* and (iv) *online authentication* of websites, and (v) services for sending *electronic registered mail*.
[1057] This involves mutual recognition of national digital identity schemes notified to the European Commission, via common *eIDAS nodes* (centralized servers) based on "SAML" technology. V. *infra*, I, Title 1, 2.2.2.1.a
[1058] Directive (EU) 2015/849 of the European Parliament and of the Council of May 20, 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 141, nº OJ L, June 5, 2015, accessed online November 24, 2021.
[1059] Directive (EU) 2015/2366 of the European Parliament and of the Council of November 25, 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 337, nº OJ L, December 23, 2015, accessed online November 24, 2021.
[1060] In practice, these *nodes* represent standardized servers that operate using a common protocol maintained by the European Commission's technical arm, *the Connecting Europe Facility*. The eIDAS-1 Regulation is thus materialized by this software ("*eIDAS nodes*") for each Member State, enabling them to exchange and synchronize trusted data on private servers (hosted by public institutions) that are compatible with each other.
V. "EIDAS-Node PRE-RELEASE version 2.6", in *CEF Digital*, more information online
[1061] *Ibid*.

In principle, this identification is unique, established with the consent of the individual[1062] , while protecting his or her privacy. This mutual recognition between Member States' trusted IT systems enables EU citizens to access cross-border public services, including via trusted service providers[1063] . However, the implementation of these electronic identification systems varies from one Member State to another. In order to benefit from this mutual recognition, an electronic means of identification must have been issued in accordance with an electronic identification scheme notified by the Member State[1064] and included on the list published by the European Commission[1065] . Since September 29, 2018, reciprocal recognition of the aforementioned means of digital identification has become mandatory[1066] . The eIDAS Regulation introduces three "*guarantee levels*" or assurance levels[1067] . These levels of confidence include precise criteria enabling Member States to compare their means of electronic identification with a Community benchmark (low, substantial and high). The latter are granted on the basis of compliance with procedures, specifications and minimum technical standards[1068] :

- A low level of security[1069] : the aim is to marginally reduce the risk of misuse or alteration of identity (identity theft).
- A substantial level of guarantee[1070] : the aim is to substantially reduce the risk of misuse or alteration of user identity.

[1062] See *infra*, II, Title 1, 2.2.3

[1063] The use of electronic certification services, such as electronic signatures, time stamps and electronic seals (*see* above), enables a trust service provider to guarantee the long-term integrity of an electronic document. These providers may be public or private technology suppliers, and are subject to the standards and controls set out in the European eIDAS standard. To carry out their activities, they must be certified and have specific technical resources at their disposal, thereby reinforcing confidence in electronic transactions within the EU.

[1064] ANSSI, "Le règlement eIDAS", in *ssi.gouv*, available online

[1065] Consult the real-time list of the 27 French trust service providers on the European Commission website at the following address

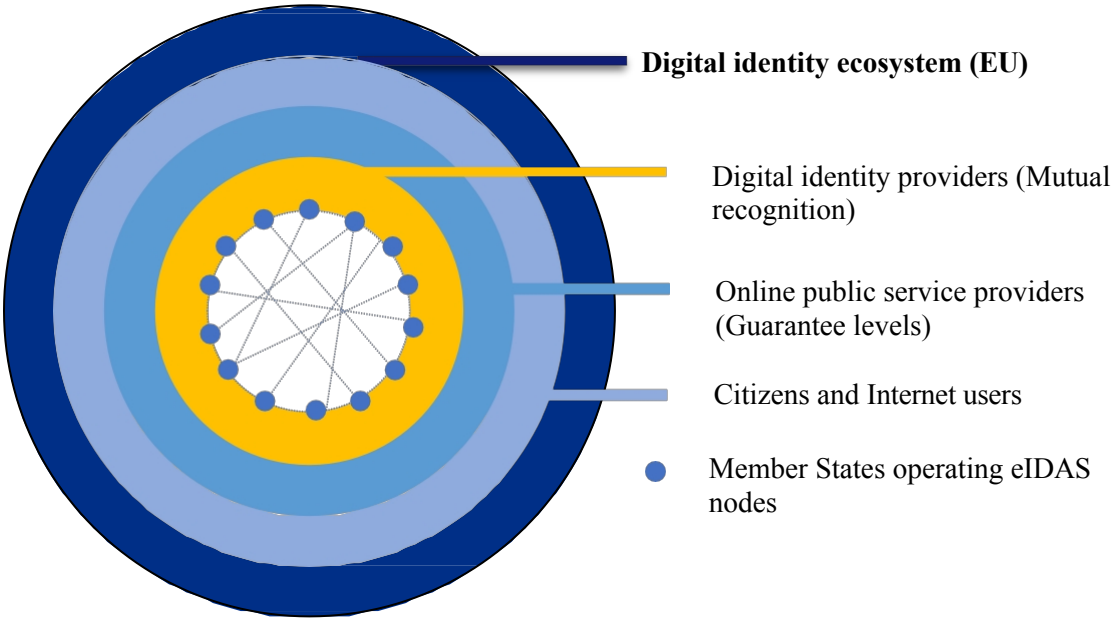
[1066] Acteurspublics.fr, "Digital identity business models", "Mutual recognition of EIMs has been effective since September 29, 2015 on a voluntary basis and will become mandatory on September 29, 2018.", p.17, accessed online on November 24, 2021.

[1067] Assurance levels must characterize the degree of trust in electronic identification means, providing assurance that the person claiming a particular identity is the person to whom that identity is attributed. V. Commission Implementing Regulation (EU) 2015/1502 of September 8, 2015 laying down minimum technical specifications and procedures relating to the levels of assurance of means of electronic identification referred to in Article 8(3) of Regulation (EU) No 910/ 2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, accessed online on 24/11/2021.

[1068] *Ibid*. Commission Implementing Regulation (EU) 2015/1502. V. Annex pp.4-14 which distinguishes each category, characteristics and design of electronic means of identification intended for natural as well as legal persons. [1069] *Ibid*. An electronic means o f identification with a low guarantee level requires: "1. [...] at least one authentication factor. 2. The electronic means of identification is designed so that the issuer takes reasonable steps to verify that it is used only under the control or in the possession of the person to whom it belongs.", p.9. [1070] *Ibid*. An electronic means of identification with a substantial guarantee level requires: "1. [...] at least two authentication factors of different categories. 2. The electronic means of identification is designed in such a way that it can be presumed that it is used only under the control of the person to whom it belongs or in his possession".

- A high level of security[1071] : the aim is to prevent any misuse or alteration of a person's identity.

Prior to the proposed eIDAS-2 amendment discussed below, eIDAS-1 did not apply to identification between private parties, but only between member states that offered electronic means of identification to citizens (public services)[1072] . However, exceptions were introduced on a case-by-case basis due to the growing demand from businesses and the private sector to extend these identification methods to civil society. As a result, many Internet users are now using 2.0 digital identification and authentication methods provided by private players, as discussed in this study.



The three levels of protection mentioned imply that state digital identity solutions are high-level by design, as they are derived from physical, regal identity documents. In Germany, for example, the law requires high-level identity verification, including a physical check imposed by the BaFIn[1073] for the opening of an online bank account. End

[1071] *Ibid*. An electronic means of identification with a high guarantee level must satisfy the substantial level in addition to having to: "1. [...] protect against duplication and manipulation and against attackers with a high attack potential. 2. The means of electronic identification is designed so that the person to whom it belongs can reliably protect it against unauthorized use".

[1072] For greater clarity, the eIDAS Regulation sets out precise requirements for the mutual recognition of electronic means of identification and electronic signatures for exchanges between public sector bodies and their users. However, it excludes internal administrative exchanges that have no direct impact on third parties, as well as private documents. The Regulation applies specifically to exchanges between the administration and the public, such as citizens and businesses, but does not apply to IT systems deemed "*closed"*, such as public blockchains (see following pages).

[1073] "BaFin reacts to N26's authentication methods", "In Germany, the law requires that identity cards be checked as a prerequisite for opening an account. This check can be carried out at a post office or branch. It is even possible to initiate the procedure through a video call", 2018, in *meilleurtauxbanques.com*, accessed online on November 24, 2021.

2022, only three countries out of 28 do not yet have an electronic identification scheme with a high level of guarantee, including France (a substantial or even high level being granted to the *FranceConnect* scheme associated with Groupe la Poste's digital identity)[1074] . In France, the Agence nationale de la sécurité des systèmes d'information (ANSSI) plays a central and indispensable role in the operational application of Article 24-1 of the eIDAS Regulation, which concerns the issuance of "*qualified certificates*"[1075] and the identification phase prior to their issue. Only four methods are currently recognized for this face-to-face or remote verification phase[1076] . ANSSI recognition is therefore essential for any player in this market, as it confers a presumption of reliability[1077] on digital identity and online identification methods that comply with its specifications[1078] . In other words, ANSSI is in a position to define the IT compliance of different identification methods, and to assign them a substantial or high level of guarantee under the Regulation. In the coming years, the proposed amendment to the eIDAS Regulation will enable full legal recognition of strong digital identity schemes derived from physical identity documents within the EU. It therefore seems important to take this factor into account in the deployment of future decentralized digital identity solutions. Article 11-1 of the eIDAS Regulation stipulates that different parties are liable for damage caused by a breach of their obligations[1079] , including the Member State, the electronic identification provider or the party responsible for the authentication procedure. This coexistence of responsibilities at different levels can make it difficult for identity and online service providers, as well as citizens and users of eIDAS-1-compliant public or private services, to understand and understand. An exception is made to this general, Community-wide responsibility when digital identity transactions are carried out on a national scale, or when a responsibility-sharing scheme is set up by the Member States[1080] . Penalties for non-compliance with the rules applicable to trust service providers are determined by the domestic law of each Member State[1081] , but at

[1074] KIROVA Marina, "Overview of pre-notified and notified eID schemes under eIDAS," eID User Community, September 13, 2019. Available at

[1075] *Qualified electronic signature certificates* attest to the identity of the natural or legal persons to whom they have been issued. Thanks to this technical recognition, the legal effect of a qualified electronic signature is equivalent to that of a handwritten signature. ANSSI, *op. cit*, "The eIDAS Regulation".

[1076] Art. 24-1-a-b-c-d. "Requirements applicable to qualified trust service providers eIDAS 910/2014", accessed online on November 24, 2021.

[1077] Art. L. 102 III du CPCE "This electronic means of identification is presumed reliable until proven otherwise when it complies with the specifications established by the national authority for information systems security, set by decree of the Conseil d'Etat.", art. L102 of the French Post and Electronic Communications Code, in *Légifrance*, consulted online on November 24, 2021.

[1078] Agence nationale de la sécurité des systèmes d'information (ANSSI). "Référentiel d'exigences de sécurité pour les moyens d'identification électronique", version of August 11, 2022, in *ssi.gouv.fr,* available at the following address

[1079] Responsibility (Electronic identification) eIDAS 910/2014, in *marchepublic.*fr, consulted online on November 24, 2021, "(i) The Member State, (ii) the party issuing the electronic means of identification or (iii) the party managing the authentication procedure, shall be liable for damage caused intentionally or through negligence to any natural or legal person as a result of a breach of its obligations".

[1080] *Op. cit.* EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, "L'identité numérique; quelle définition pour quelle protection?", *op. cit*, "Le règlement ne s'applique pas pour les transactions nationales et les États membres peuvent prévoir un régime de partage de responsabilité différent", p.132.

[1081] Art. 16 Sanctions (Trust services) eIDAS 910/2014. (2014), in *marche-public.fr*. Available at

To date, no binding provisions have been established to penalize the provision of non-qualified services within the meaning of eIDAS.

The eIDAS Regulation, which has been aiming to create a European digital identity for several years[1082] , is currently being revised[1083] , as it has been facing certain limitations for seven years[1084] . Only 60% of the EU population, i.e. more than 14 out of 28 member states, can use their national digital identity systems across borders. Also, only 14% of major public service providers in all member states allow cross-border authentication using an electronic identity system. While at least 14 Member States already have an eID card or are in the process of developing one, there is still relative uncertainty as to their compatibility and interoperability. In addition, most member states do not have fully operational eIDAS[1085] nodes, which limits the possibility of cross-border authentication. In addition, the eIDAS-1 infrastructure is centralized and presents several IT vulnerabilities as identified in 2019[1086] , raising questions about its long-term resilience. For this reason, some specialists are proposing the use of blockchain technology to improve the interoperability and security of the eIDAS infrastructure. We therefore need to study blockchain's compliance with the eIDAS Regulation and determine how it could meet the legal and technical requirements of the Regulation. For blockchain technology to be at the heart of this infrastructure already in use, this would require a legal overhaul, as explained in a report in 2021 by several experts commissioned by the Ministry of t h e Interior[1087] . In this sense, the provisions concerning trust services in the

[1082] *Op cit*, "Communication Shaping Europes Digital Future", accessed December 6, 2021, p.6, free translation from English, "A universally accepted public electronic identity (eID) is needed so that consumers can access their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily share personal data with them."

[1083] Reference is made to the launch of a consultation process in July 2020, followed by the draft proposal for an amending Regulation published in June 2021. The final version of the "*eIDAS-2*" text should be adopted in the first quarter of 2023, v, next section.

[1084] As Me Alain Bensoussan explains: "[...] all these players [in the digital identity sector] are today absolving themselves of any responsibility by taking refuge behind an obligation of means, and that the eIDAS regulation, despite the hopes raised, has been able to do nothing other than promote the interoperability of "means" (the Devices) and select existing standards (also "means") for the mutual recognition of [identity] Assertions.", *op. cit.*
"Digital Identity 5.0".

[1085] These *nodes* represent standardized servers that operate with a common protocol maintained by the European Commission's technical arm, the *Connecting Europe Facility*.

[1086] *Op. cit.* EYNARD Jessica, et al. "All that was required was to make a malicious connection to a Member State's eIDAS Node server and provide false certificates during the initial authentication process*"*, p.127.

[1087] *Op. cit.* COUTOR Sophie et al, "Blockchain et identification numérique - Restitution des ateliers du groupe de travail 'blockchain et identité'", 2020, available at: "[...] the eIDAS framework is too limited to integrate blockchain. Intended to frame the provision of a set of determined attributes (the minimum set of mandatory attributes that identify the person, or "pivot identity") defined in the 2015/1501 implementing act, eIDAS allows: (i) data minimization and selective disclosure of attributes, (ii) the use of anonymized credentials such as Verifiable Credentials based on the W3C data model, (iii) the communication of related identifying attributes, other than "pivot data" (which, referring to legal identity, serve to identify the person), (iv) nor online services offered by the private sector, (the Regulation deals only with the action of public administrations), (v) nor the secure hosting of personal data on a mobile personal device [PIND]. ", p.83.

eIDAS Regulation[1088] do not seem to allow for a favorable interpretation of blockchain technology. Firstly, in order to be accessible to another member state, a public online service using blockchain technology would have to meet the requirements of the Regulation and be assigned one of the three levels of trust mentioned. While the Regulation's approach is technologically neutral, it would eventually enable the qualification and legal recognition of 3.0 technologies, particularly with regard to the level of guarantee they can legitimately inspire as a trust service, which is what eIDAS-2 proposes[1089] . By way of illustration, eIDAS-1 does not currently govern the case where a private entity (company) issues a DID/VC to a natural person for use in his or her private sphere. It has been noted that certain use cases are covered by eIDAS, notably those involving the public sector and services for citizens, as already demonstrated by EBSI's activities in France and within the EU. In this respect, it seems that private blockchains[1090] and public[1091] are not covered by eIDAS, as it does not apply to trust services provided exclusively in closed systems. Private blockchains, which in principle are only accessible to one actor, and public blockchains, which do not comply with this text as they do not involve transactions linked to digital identities, therefore do not seem to be concerned. Hybrid blockchains, on the other hand, are directly targeted by the eIDAS regulation. This is demonstrated by the European Blockchain System (EBSI), in which each member state operator, and ultimately its companies, will qualify as a trust service, leading to legal recognition of these hybrid technologies, which will eventually also include some of the decentralized digital identity standards discussed above (see next section).

When it comes to the degree of trust placed in a person's digital identity online, and with regard to the three levels of assurance mentioned above, current decentralized identity implementations aim to be recognized with a specified level of assurance as substantial or high, when coupled with other traditional online identity verification mechanisms (having to be equivalent to physical identity verification as mentioned with the German example). A secure infrastructure running on blockchain technology could gain credibility by being qualified as a

[1088] Art. 16.a)b)c) and 17 "Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", OJ L, 2014, accessed online on November 24, 2021.
[1089] See next section.
[1090] In principle, private blockchains do not appear to be subject to the rules of the eIDAS Regulation, as only authenticated and authorized users can carry out transactions and access this electronic registry. Only miners, who are identified and enrolled validator nodes, have the ability to update the registry and its related governance charter, as well as other legal components such as the consortium's general terms of use, non-competition charter, articles of association or partnership agreement. It is stressed that peer recognition of such closed or at best semi-open systems seems difficult to reconcile with the principle of mutual recognition imposed by eIDAS-1 (unlike open blockchains, where it is simpler to know whether compliance exists or not, as their systems are accessible). However, eIDAS-2 indirectly favors closed and hybrid systems, as discussed below.
[1091] In principle, public blockchains are also outside the scope of eIDAS-1, as anyone can submit transactions and access the registry. Because anyone can deploy a validator node and submit a new block that can complete the registry, and get involved in the governance of this public blockchain, then the eIDAS rules originally designed for trusted third parties and services, can only with difficulty find application.

trusted service within the meaning of the aforementioned Regulation. In 2022, decentralized identity solutions are gradually being considered as quality service offerings for businesses and citizens, due to their many technological and legal advantages. Since 2020, two main solutions have been considered to offer legal recognition to decentralized identity. Firstly, several recommendations and scenarios described in the report on decentralized identity and eIDAS, published in April 2020 by Doctor of Law Ignacio Alamillo Domingo[1092] , could be implemented by the European legislator. In 2023, these recommendations are included in the proposed eIDAS-2 amendment described in the following section. It was also proposed to refer to the "*eIDAS Bridge*" initiative[1093] to add legal fundamentals to trust services providing verifiable attestations, in addition to the use of electronic certificates and conventional electronic seals within the meaning of eIDAS-1.

While since 2016, the eIDAS Regulation has enabled a holistic transformation of public sectors and their trust services, the framework for digital identity within the European Economic Area remains fragmented and poorly harmonized. Two observations can be made. Firstly, the current version of the Regulation is a source of uncertainty in the face of rapidly expanding needs for digital identities, in terms of privacy, IT security and ease of use. Given the difficulties encountered in adopting and implementing the initial version of eIDAS, the European Commission has recognized the need to reassess its European digital identity policy, and has proposed the eIDAS-2 amendment explained below. Indeed, the EU is positioning its businesses and institutions at the heart of a new strategy of data openness and interoperability between its member states. Secondly, new technological opportunities are emerging in the short term, such as the use of blockchain systems, which will open up new economic and social possibilities. As a result, the EU is attempting to establish a new legal consensus through eIDAS-2, drawing on the new IT interoperability enabled by decentralized digital identity, and to prevent consumers from continuing to use private sector digital identity 2.0 alternatives, which are sometimes not eIDAS or RGPD compliant. The ultimate goal of a decentralized digital identity, already widely adopted by some IT specialist communities, is to enable the creation of verifiable credentials (VCs) derived from national digital identity documents and their national certificates (such as the CNIe or the online-compatible driving license). However, there are still a number of obstacles to the advent of liberated, trusted and partially decentralized digital identities.

[1092] Dr. ALAMILLO DOMINGO Ignacio, "SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market (B-1049 Brussels)", *op. cit.* available at [1093] *Ibid*. p.105.

2.1.1.1.a The revised eIDAS Regulation (eIDAS-2)

On June 03, 2021, Margrethe Vestager, Executive Vice President of the European Commission, will "*A Europe fit for the digital age*"[1094] announced the creation of a European digital identity that would enable citizens to move around and carry out identity transactions online in any member state at no extra cost and with complete confidence[1095] . This political will was followed by a proposed amendment to modify the eIDAS Regulation and establish a European framework for digital identity eIDAS-2[1096] , based on the evolution of user expectations in terms of identity data control and the growth of the digital market[1097] . The aim of this amendment is to provide a European digital identity that is interoperable and recognized on a voluntary basis for all citizens and businesses in the euro zone[1098] . This new European political and legal strategy is based on three main pillars. The first pillar aims to improve the effectiveness of mutual recognition systems for national digital identification schemes (eIDAS-1). The second pillar aims to enable the private sector to offer services based on enhanced digital identification (partially 3.0) and complying with a high level of guarantee. Finally, the third pillar aims to provide a "*European digital identity wallet*"[1099] of trust, enabling the storage and use of unique, interoperable attributes under the sole control of the user. As these functionalities are by design made possible by the decentralized digital identity (IND), previously studied, this European digital identity wallet can thus be considered as a decentralized digital identity wallet (PIND) in the sense of the present study. Although the eIDAS-1 Regulation has been effective in providing a high level of trust and encouraging the adoption of trust services, it has failed to meet new market demands in terms of new technologies and the increasing digitization of European citizens' daily lives[1100] . Lack of notified e-identity solutions in all countries

[1094] *Op. cit*. European Commission (EC), "A Europe fit for the digital age", 2019, available online

[1095] European Commission (EC), "The Commission proposes a reliable and secure digital identity", in *Press Corner*, accessed online November 25, 2021, "The European digital identity will enable us to act in any Member State as we would at home, at no extra cost and more easily, whether to rent an apartment or open a bank account outside our country of origin. And all in complete security and transparency. So it will be up to us to decide what personal information we want to share, with whom and for what purpose [reference to IND]. This will give us a unique opportunity to deepen our understanding of what it means to live in Europe and to be European".

[1096] *op cit*, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards the establishment of a European framework for a digital identity, available at

[1097] Reference is made to the launch of a consultation process (in July 2020 and then to the draft proposal for an amending Regulation published in June 2021, available at the following address. The final version of the "*eIDAS-2"* text should be published and adopted in the first half of 2023.

[1098] *Ibid,* "Explanatory memorandum, Background to the proposal, Results of ex-post evaluations", 3: "The vast majority of e-identity and remote authentication needs are in the private sector, particularly among players in areas such as banking, telecommunications and platform operation, who are required by law to verify the identity of their customers. The added value of the eIDAS regulation with regard to electronic identity is limited due to its low coverage, adoption and use".

[1099] *Ibid,* "2. Legal basis, subsidiarity and proportionality. Fundamental rights".

[1100] CE, "Shaping europe's digital future", 2020, accessed online September 15, 2021, p.6,
"A universally accepted public electronic identity (eID) is needed so that consumers can access their data and securely use the products and services they want without having to use unrelated platforms to do so and unnecessarily share personal data with them."

The European Commission's decision to propose the eIDAS-2 amendment was prompted by the fact that eIDAS is not yet fully compliant with member states' legislation, and lacks the flexibility to support new digital uses. In addition, digital identity 2.0 solutions not covered by the scope of eIDAS-1[1101] raise concerns about the protection of users' privacy and data. eIDAS-2 is therefore in line with the priorities for digital transformation set out in the EU's strategy for the digital economy.

"*Shaping Europe's Digital Future*"[1102] and contributes to achieving the objectives set out in the "*Digital Decade for Europe: digital targets for 2030*"[1103] . This proposal aims to support the EU's transformation towards a digital single market by proposing measures for public authorities, citizens and online service providers. What's more, the Regulation is mandatory and directly applicable in all EU member states. While eIDAS-1 has helped to resolve certain issues relating to the legal qualification and technical framework of digital identity within EU countries, eIDAS-2 undoubtedly gives new legal recognition to decentralized digital identity[1104] and blockchain technology[1105] . The concrete ambition of this amendment is to increase the use of national digital identities under eIDAS-1 from the current 60% to 80%[1106] by 2030. This objective is all the more ambitious in that it faces a very short implementation time of around three years (2023-2026), as summarized prospectively in the following timeline:

[1101] This refers to the solutions offered by GAFAM/BHATX and certain financial institutions. Their "*Single sign-on - SSO*" or "*All-in-one authentication*" solutions enable users to navigate between several online services without re-registering for each of them, but simply by quickly authenticating themselves thanks to a federated digital identity solution (this highly popular solution, however, relies on the massive and opaque collection of users' personal data). Indeed, these *SSO* solutions are subject to new computer attacks that can easily mislead their users, *see supra,* I, Title 1, 2.2.1.1.

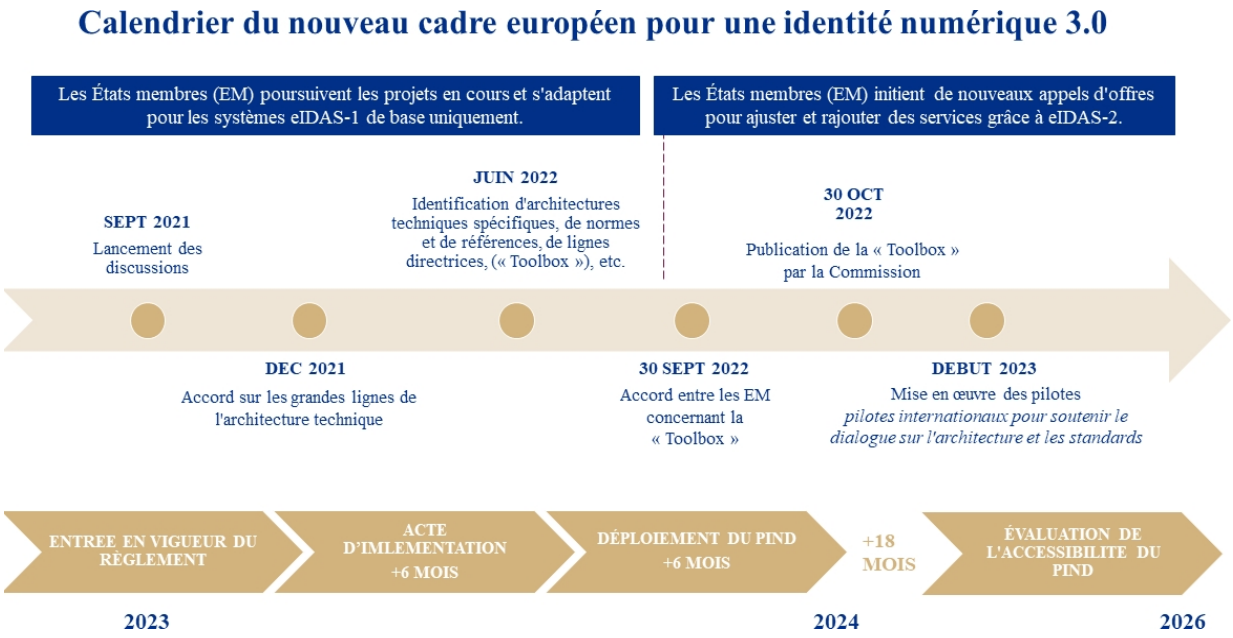
[1102] European Commission (EC), "Shaping Europe's digital future. Building Europe's digital future", available at the following address

[1103] EC, "Europe's Digital Decade: digital goals for 2030", *op. cit.* available at the following address

[1104] The amendment designates verifiable attestations (VC) as "an attestation in electronic form that enables the authentication of attributes" or "electronic attestation of attributes". Moreover, a qualified electronic attestation of attributes is, in the sense of this Regulation, required to be "issued by a qualified trust service provider", *op. cit*., (45). For reasons of intelligibility, we have retained the use of the term "verifiable attestation", which is likely to be the term most widely used by the ecosystem we have described.

[1105] The amendment neither names nor cites a blockchain technology as such, but prefers to use the term "electronic ledger" for the sake of technological neutrality. In this sense, Article 1 of eIDAS-2 defines an *electronic ledger* as "a tamper-proof electronic record of data, ensuring the authenticity and integrity of the data it contains, the accuracy of the date and time of that data, and its chronological classification". While this ambivalence may refer to all types of electronic registers, whether *centralized*, *decentralized* or *hybrid*, we note that the European legislator's intention is to enable the qualification and subsequent legal recognition of blockchain technologies (private and hybrid) by including them in this broad definition. In March 2023, this section 11 dedicated to electronic registries was removed from the text. In reaction, an open letter from the ecosystem was signed by over 200 blockchain technology specialists. INATBA, "Open Letter for the preservation of the Electronic Ledger's provisions in eIDAS 2", in *inatba.org*, available at

[1106] EC, "Commission proposes a trusted and secure Digital Identity for all Europeans", "[...] by 2030, all key public services should be available online [...] and 80% of citizens should use an electronic identification solution", in *Press Corner*, accessed online June 3, 2021.



Faced with the adoption of this proposed amendment to the eIDAS Regulation, expected by September 2023, it is possible to summarize its cardinal points, particularly in relation to Web 3.0. Firstly, three new categories of qualified trust services have been added to the five already enshrined in eIDAS-1[1107] , namely, electronic archiving services[1108] , the management of devices for the creation of remote electronic signatures and stamps[1109] and electronic registers (including blockchain)[1110] . As a result, from the first half of 2023, a date to which we must add 18 to 24 months for the implementation of certain technological standards by member states, eIDAS-2 will provide a framework for around ten trust services, and will enable the use of multiple 2.0 and 3.0 technologies. A presumption of reliability and authenticity would thus be conferred on

[1107] *See* previous section: (i) Signature for natural persons, (ii) electronic stamps for legal entities, (iii) electronic time stamping, (iv) online authentication of websites and (v) electronic registered mail services. Finally, eIDAS-1 & 2 now provide a legal framework for 10 electronic usages widely adopted or in the process of being adopted on the Internet, as mentioned in the first article of the eIDAS-2 proposal: "a legal framework governing electronic signatures, electronic stamps, electronic time stamps, electronic documents, electronic registered mail services, certificate services for website authentication, electronic archiving and electronic attestation of attributes, management of remote electronic signature and electronic stamp creation devices, and electronic registers".

[1108] *An electronic archiving service* is considered to be "a service ensuring the reception, storage, deletion and transmission of electronic data or documents in order to guarantee their integrity, the accuracy of their origin and their legal particulars for the entire duration of their preservation", *see* definitions and Section 10, art.45g.

[1109] Art. 3. 14: "'electronic signature certificate' means an electronic attestation or set of attestations which associates the validation data of an electronic signature with a natural person and confirms at least the name or pseudonym of that person" and art. 3. 29: "'electronic seal certificate' means an electronic attestation or set of attestations which associates the validation data of an electronic seal with a legal person and confirms the name of that person".

[1110] Freely translated from the English term "*Electronic Ledgers*", Section 11 & Recital (34): "This trust service is necessary to avoid fragmentation of the internal market, by defining a single pan-European framework enabling cross-border recognition of trust services that support the operation of qualified electronic registers [closed blockchains]. Data integrity, for its part, is very important for the pooling of data from decentralized sources, for autonomous identity solutions [IND], for the attribution of ownership of digital assets, for the recording of business processes for the purpose of verifying compliance with sustainability criteria and for various use cases on capital markets.".

qualified electronic registers: "*a qualified electronic register benefits from the presumption of the uniqueness and authenticity of the data it contains, the accuracy of its date and time, and its sequential chronological order within the ledger*"[1111] . The conditions for an electronic ledger to be considered qualified are as follows: (i) it must emanate from one or more trust services[1112] , (ii) it must guarantee the uniqueness, (iii) authenticity of the data and transactions recorded, as well as (iv) the chronological order and (v) the correct date and time of the information. Finally, he must record the data in such a way that any subsequent modification of the data is immediately detectable. With regard to online identification and authentication, new "European *Digital Identity Wal*lets*" (EDIW*)[1113] will be developed and proposed by member states by early 2024, as suggested in the previous frieze. These decentralized digital identity wallets (PIND, already mentioned), this time European, will be made available to EU citizens, residents and companies (natural and legal persons) wishing to identify themselves or provide confirmation of certain personal information[1114] . They can be used online and offline[1115] to access public and private digital services[1116] , including across borders (interoperability) in all EU member states. These identity cases will have to support large sets of electronic attributes (qualified or unqualified VCs), which was not the case with the initial version of the eIDAS Regulation[1117] , while enabling "*selective disclosure*" of identity attributes[1118] as well as "*qualified electronic signatures*" functionality[1119] , for example to facilitate the political participation of European citizens (e.g. online voting, referendums)[1120] . Each identity case

[1111] Section 11, art. 45 nonies, available online
[1112] Art. 3. 16. and Annex V and VI of the eIDAS-2 Regulation (Requirements applicable to electronic attestations qualified by attributes & minimum list of attributes).
[1113] Art. 6 bis. Translation by "digital identity briefcase" is also possible, see also "Proposition d'une taxonomie francophone pour l'identité décentralisée". 2021. ⟨hal-03398096⟩.
[1114] These identity cases, or PINDs, will have to "enable users to store identity data, supporting documents and other personal information in a single place".
attributes to provide them on demand to relying parties and use them for online and offline authentication and to create electronic signatures and seals", (i) (42).
[1115] Each PIND must enable direct, peer-to-peer communication (i.e. without third parties) between the PIND holder (user) and a verifier (online service). This communication can take place both online (via an Internet connection) and offline (via QR code, Bluetooth, SMS, etc.).
[1116] Contrary to its first rather restrictive version for private services, this amendment to the Regulation thus allows private services to provide digital identities (with strong authentication) to individuals, within the meaning of a list as defined: "Private stakeholders providing services in the fields of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of European digital identity portfolios for the provision of services where strong user authentication for online identification is required by national or Union law or by contractual obligation. "(28) available online
[1117] *Op. cit.* v. Explanatory memorandum 1: "[...] the current eIDAS framework does not cover the provision of electronic attributes". the eIDAS regulation does not allow users to limit the sharing of identity data to what is strictly necessary for the provision of a service".
[1118] Results of ex-post evaluations and impact assessments, "[...] allowing users to choose when and with which private service provider to share various attributes, depending on the use case and the security required for the transaction concerned."; (29) "EDIW should technically enable the selective disclosure of attributes to relevant parties.".
[1119] Art. 6 bis. 3.(b), Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards the establishment of a European framework for a digital identity, available at
[1120] Explanatory Memorandum, 1: "The portfolio will also provide qualified electronic signatures that can facilitate participation in political life. *v. infra*, I, Title 2, 2.2.7

national digital identity card will also be free[1121] and optional for European citizens. In addition, it has been noted that all providers of "*qualified electronic attributes*" (DID, VC) must provide these services via a legal entity distinct from the one they use for their PIND, in order to avoid the risks of aggregation or theft of said identity attributes.

Member States must provide[1122] and then notify[1123] of at least one PIND with a high level of security and guarantee[1124] , no later than twelve months after eIDAS-2 comes into force, i.e. by September 2024[1125] . In this way, Identity Providers will provide verifiable attestations that are compatible between each PIND. This opens up a new possibility for European countries to accept new types of credentials that are electronically and legally cross-border, interoperable and secure (including with non-EU countries, thus moving towards a first form of universal digital identity[1126]). Indeed, eIDAS-2 refers to this possible international recognition of European verifiable attestations[1127] , a significant step forward for digital identity, which is thus less dependent on the conclusion of countless legal agreements in order to multilaterally recognize digital identity solutions. However, the proposal explains that "a *process of close and structured cooperation between the Commission, the Member States and the private sector is necessary*"[1128] . To this end, a "Toolbox" proposes the implementation of an IT architecture based on common standards and practices that member states will have to respect for their PINDs. In this respect, they will have to (i) enable the provision and exchange of identity attributes (VC, DID), (ii) ensure the functionality and security of PINDs or (iii) set up governance or study their dependencies on identity attribute providers. The European Commission is also introducing "*Codes of conduct*"[1129] to facilitate the provision and use of PINDs. These codes of conduct will be drawn up within twelve months of the adoption of eIDAS-2, and will then be implemented.

[1121] Art. 6a.
[1122] Introduction of an obligation for Member States to issue a digital identity wallet no later than 12 months after the amendment enters into force (article 6a 1.), see below.
[1123] Member States will have to notify their EDIW/PIND in accordance with Art. 6a2, *op. cit.* Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards the establishment of a European framework for a digital identity. Available at the following address
[1124] Art. 6 bis. 4.(c).
[1125] "In order to ensure that all natural and legal persons in the Union have secure, reliable and continuous access to cross-border public and private services, each Member State shall issue a European digital identity wallet within 12 months of the entry into force of this Regulation.
[1126] See *supra*, I, Title, 1.1.3.2.
[1127] *Ibid.* Legislative financial statement, 1.4.4. Performance indicators. "Increase cross-border recognition and acceptance of electronic identification schemes, with the ambition of achieving universal acceptance".
[1128] Art. 36.
[1129] (28) "Self-regulatory codes of conduct at Union level ("codes of conduct") should be developed in order to contribute to the widespread availability and ease of use of electronic means of identification, including European digital identity wallets, under this Regulation. Codes of conduct should facilitate widespread acceptance of electronic means of identification, including EDIWs. They should be drawn up within twelve months of the adoption of this Regulation".

implementation within eighteen months[1130] . These codes of conduct will also have to incorporate ethical components, which this research dedicates in a section[1131] . What's more, responsibility for these European identity kits (PINDs) lies with the member states[1132] and their labeling will not be subject to "*peer review*" processes[1133] as required by eIDAS-1. A member state must provide a common interface for users and citizens to enable easy interaction between online services and this interface. To this end, a European "*trust mark*"[1134] for the European Digital Identity Portfolio ("*Trust Mark*") has been introduced. A list of certified PINDs has also been drawn up and is kept up to date by the European Commission[1135] . It should be noted that a PIND has the effect of imposing itself on large online platforms or "*Gatekeppers*"[1136] under eIDAS-2. Some private service providers, whose activities are essential to civil society, will thus be obliged to offer and accept these state PINDs or, failing that, to implement high-level authentication for their users[1137] . In this respect, it is likely that some large technology companies will decide to develop their own PINDs with a high level of guarantee, not only because these decentralized applications can support multiple use cases, opening up a new field of possibilities in commercial terms, but possibly also to escape this attempt by the EU to impose a sovereign European PIND.

[1130] Section III, (16), 4: "These codes of conduct shall ensure that electronic means of identification, including European digital identity wallets [...] are accepted in particular by service providers who rely on third-party electronic identification services for user authentication. The Commission shall facilitate the development of these codes of conduct in close cooperation with all interested parties and shall encourage service providers to complete the development of the codes of conduct within twelve months of the adoption of this Regulation and to effectively implement them within eighteen months of the adoption of this Regulation".

[1131] See *infra* II, Title 2, 1.1

[1132] PINDs must be "*issued*" or "*approved"* by other member states, which has implications in terms of liability: a state may thus be held liable in the event of a personal data breach stemming from its *national digital portfolio*, art.10a, available at

[1133] Possibility of relying on certification to guarantee compliance with the Regulation as an alternative to the peer review process: INDPs will be assessed by reference to "common technical standards and references" and will therefore be recognized equally within the European Union, in accordance with art. 42 of the RGPD

[1134] "'EU digital identity wallet trustmark' means an indication formulated in a simple, clear and recognizable manner that a digital identity wallet has been issued in accordance with this Regulation", art.1. 3.(i) 49.

[1135] Art. 6 quinquies, "the Commission shall draw up, publish and update a list of certified European digital identity portfolios", available at the following address

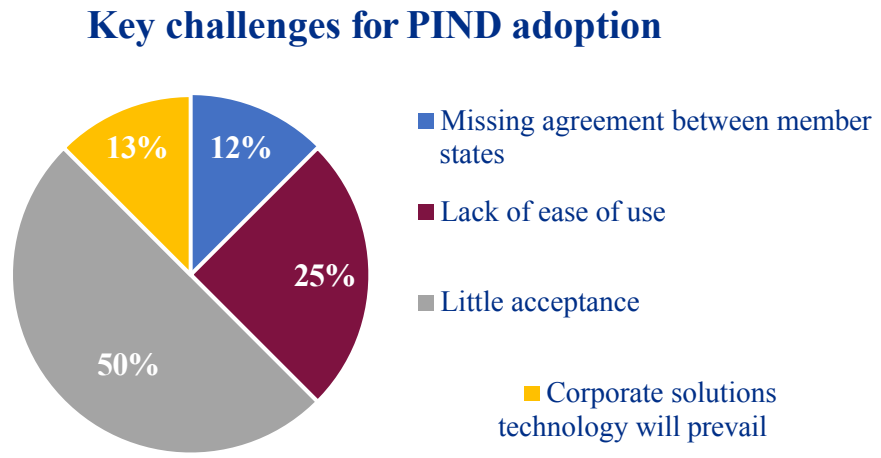
[1136] "Where very large online platforms require users to authenticate themselves to access online services, these platforms should be required to accept the use of European digital identity wallets at the voluntary request of the user. Users should not be required to use the wallet to access private services, but, where the user so wishes, very large online platforms should accept that the European digital identity wallet be used for this purpose, in compliance with the principle of data minimization", recital (28).

[1137] Large platforms such as Amazon, Google or Facebook will be obliged to accept the use of EU digital identity portfolios at the user's request (e.g. to prove age). *Ibid.* "Private user parties providing services in the fields of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of European digital identity wallets for the provision of services where national or Union law or a contractual obligation require strong authentication of users for online identification purposes".

In terms of personal data protection, the use of data (consultation, sharing or revocation) must be possible directly by the user[1138] . This security and selectivity of the data that the user chooses to share would, according to this study, reinforce certain fundamental rights[1139] . The issuer of a PIND must be able to ensure "*unique identification*" of users. By design, the PIND issuer should not be able to combine identification data with personal data from other services (unless requested by the user)[1140] . Also, a physical separation of technological and software bricks (2.0 & 3.0) must be applied in the face of other types of data[1141] . In this respect, suppliers of hardware peripherals such as mobile operators are obliged to offer this separation via a "*secure element*". For such functionality to be possible on every citizen's device and compatible with his or her sovereign PIND, this implies that all manufacturers of electronic peripherals (telephone and computer manufacturers, etc.)[1142] implement these components in their products right from the design stage. Such a process seems essential, though complex and costly, which could complicate the implementation of this rule, which would then only be partially complied with in the short term. To date, PINDs only offer cryptographic keys connected to servers, and do not yet take advantage of the security benefits offered by a hardware component directly integrated into European citizens' devices (such as the French CNI, which integrates several secure chips, as already mentioned). A

[1138] Recital (29): "European digital identity portfolios should technically enable selective disclosure of attributes to user parties. This functionality should become a basic design element, thereby enhancing service convenience and personal data protection, particularly with regard to minimizing the processing of personal data".
[1139] V. Results of the ex-post evaluations, Fundamental Rights, "By using the European digital identity portfolio, the user will be able to exercise control over the amount of data provided to user parties and be informed of the attributes that will be required for the provision of a particular service", *see infra*, II, Title 1, 2.2.
[1140] The issuer of portfolios may not collect data on the use of portfolios unless it is necessary for the operation of the portfolio, in accordance with art. 6bis, 7: "The entity issuing the European digital identity portfolio shall not collect information on the use of the portfolio that is not necessary for the provision of the related services".
[1141] In other words, a restricted combination of users' personal data must be ensured by its supplier: the supplier of a PIND will not be able to combine identification data with personal data from other services (unless the user so requests).
[1142] The eIDAS-2 amendment requires a secure *hardware element* to store each user's cryptographic keys. This secure, integrated element can be on a SIM card, or via other methods such as NFC, Bluetooth, etc.

A similar observation applies to biometric authentication, which is also favored by eIDAS-2[1143] .



With the adoption of eIDAS-2, an online service (public or private[1144]) that uses blockchain technology could be accessible and legally recognized as a trusted third party within the EU. A decentralized identity solution deployed by a Member State would also be assigned one of the three levels of trust initially instituted by eIDAS[1145] . With regard to the legal recognition granted to "*qualified electronic attestations*", eIDAS-2 defines them as a characteristic, i.e. the quality of a natural or legal person in electronic form. The similarity between this definition and that of "*verifiable credentials - VCs*", studied previously and specific to the decentralized identity model according to the W3C, is striking and undoubtedly linked. A signed and qualified verifiable credential within the meaning of the modified Regulation guarantees legal enforceability against its holder, thanks to the traceability and integrity of its source, i.e. the service and trusted third party to which it is linked. However, not all attributes managed by a PIND will be qualified in the sense of eIDAS-2, as is the case for VCs issued from self-sovereign digital identities (INAS). This means that certain digital environments will be more conducive to the use of unqualified attributes, such as the[1146] metavers studied in part two, and more specifically any particularly decentralized segment of Web 3.0. This verification of the authenticity of attributes with their trusted sources and third parties seems essential for use cases linked to the civil and primary identity of citizens. Indeed, this European digital identity will be rather hybrid, i.e. it will include both centralized and distributed (i.e. semi-decentralized) components. The use of qualified trust services to

[1143] Recital (11), "The use of biometric authentication is one of the identification methods offering a high level of trust, particularly when used in combination with other authentication elements.".
[1144] And not simply public, as in the current version of the eIDAS-1 Regulation, which strongly limits electronic identification services to public services.
[1145] Current decentralized identity implementations aim to be recognized with a level of assurance specified as at least *substantial* (in the short term) and if possible *high* (in the medium and long term).
[1146] See *infra*, II, Title 2, 1.4

By extension, issuing VCs that are also qualified in the sense of one Member State will ultimately enable them to be mutually recognized in any other Member State[1147] . In legal proceedings, for example, these 3.0-qualified attributes cannot be denied legal effect and admissibility as digital evidence simply because they are in electronic format. Indeed, eIDAS-2 recognizes and presumes the cryptographic reliability of the sources and interactions of each of these attributes, notably through the use of hybrid or private blockchains recognized as trust services. It is therefore envisaged that a qualified verifiable certificate will produce the same legal effects as physical certificates legally issued on paper[1148] . However, the rules governing the issue, format, operation and interoperability of these attestations have not yet been specified[1149] . They will have to be defined by the Member States as part of the toolbox program that began in September 2021.

The new section 11 dedicated to "*qualified electronic registers*" (blockchains) enshrines the presumption of uniqueness, authenticity and immutability of the data contained therein. Definitions of the implementing acts and delegated acts for eIDAS-2 will begin in 2023. These acts will specify the regulatory and technical frameworks with regard to the sector-specific features of certain markets and services (health, transport, driving licenses, border control, means of payment and financial transactions, diplomas, certifications or attestations linked to the education or training of individuals). This "*presumption of reliability*" relates to the traceability, time-stamping and integrity of operations concerning identity data, for example. Companies operating a private or hybrid blockchain will therefore be able to request that it be certified, i.e. qualified as a trust service[1150] . This coverage is positive for the Web 3.0 community as a whole, and particularly for the IND, which will be able to rely on multiple private or hybrid blockchains whose data and transactions will be officially recognized as trusted at both national and European level, and perhaps internationally in the long term. Nevertheless, the first step is to ensure that the previous version of eIDAS-1 nodes is compatible with the version that will be updated by eIDAS-2, enabling the implementation of blockchain technology - such as EBSI, mentioned in the first section of this study - and the concept of a partially decentralized European digital identity. Secondly, the obligation to provide a PIND is closely linked to electronic identification schemes, whose notified guarantee level must be high[1151] , which means that

[1147] Art. 45 bis. Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards the establishment of a European framework for a digital identity, available at

[1148] Recital (27): "General requirements should be established to ensure that an electronic attestation qualified by attributes has a legal effect equivalent to that of attestations legally issued on paper. However, these requirements should apply without prejudice to Union or national law defining additional specific sectoral requirements as regards the form having underlying legal effects and, in particular, the cross-border recognition of electronic attestations qualified as attributes, where applicable.".

[1149] Art. 45(c) and 45(d), *op. cit,* Proposed Regulations.

[1150] In accordance with art. 24 of eIDAS-1

[1151] Section 1, (7), 6. European digital identity portfolios are issued under a notified 'high' guarantee level electronic identification scheme". In practice, this is likely to pose difficulties for certain Member States whose notified electronic identification scheme is not yet recognized as being of a high level.

This is not yet the case for France, whose electronic identification scheme has a substantial guarantee level as of April 2023[1152] . In other words, France must issue an electronic identification scheme with a high guarantee level in order to be able to issue its PIND.

Furthermore, the eIDAS-2 amendment seems to reinforce the complementarity with certain financial regulations studied earlier (MiCA, TFR, Data Act). For crypto-assets, these interlocking regulations (including eIDAS-2) will have the effect of socially and informatically recentralizing[1153] their decentralized protocols and ecosystems, particularly where public blockchains are concerned. These legal rules thus emanate from and are articulated through political and sometimes social pressure on these Web 3.0 ecosystems. In concrete terms, law and certain technologies seem to be reused to better identify each actor and each interaction within various economic, social and financial value chains[1154] . In other words, eIDAS-2 will reinforce a form of indirect centralization through the identification of Web 3.0 actors, in the same way as other regulations (MiCA, TFR), albeit under the guise of other legal rules and political motivations, which are all converging (against public blockchains). While technological neutrality seems to be partially respected by these texts in law, with eIDAS-2, exchanges of qualified electronic attributes will only take place in an IT circuit that is actually rather closed, i.e. mostly circumscribed between trusted service providers. It's more a question of semi-opening up these qualified electronic attributes than of opening them up completely, as the European Commission may suggest in this amendment and its technological and literal references, for example by using the term "*universal*" five times. In the sense of the aforementioned legal rules imposed by eIDAS-2, it appears that public blockchains (Bitcoin, Ethereum) will never be able to become trust service providers, i.e. fulfill the conditions for certification of trust service providers, which are centralized. This means that they will not benefit from the aforementioned legal recognition (presumption of reliability) that private and hybrid blockchains do. Consequently, there seems to be a new attempt to de-institutionalize - through the law - the current social adoption of open blockchains, in favor of closed blockchains, supposedly more protective of rights and efficient[1155] in all fields according to certain political, institutional or even governmental communications and communicators. As a result, eIDAS-2 seems to indirectly encourage this fight against the pure decentralization of certain public blockchains, which, according to this study, is harmful.

[1152] Check for updates concerning France, according to the official EC list, available at the following address
[1153] V. Appendix 7.
[1154] Recital (31), "Secure electronic identification and the provision of attribute attestations should offer greater flexibility and solutions to the financial services industry with regard to customer identification and the exchange of specific attributes necessary to comply [...] anti-money laundering regulations [TFR] and suitability requirements arising from investor protection legislation [MiCA], or to enable compliance with strong customer authentication requirements for login and transaction execution in the field of payment services".
[1155] V. Appendix 6, Focus 3.

for all Web 3.0 players, including, paradoxically, closed blockchains, provided this hypothesis is confirmed in the future. Indeed, hybrid and private blockchains derive much of their technological innovation from public blockchains, which have much larger developer communities and sources of innovation, as noted in several previous parts and Annexes of this research[1156] . Moreover, this lack of legal recognition seems paradoxically to lead to confusion with regard to the textual use of the term "*immutable*"[1157] in reference to PINDs, which will therefore be based on private or hybrid blockchains that are centralized and therefore mutable, as only a few blockchains are computationally highly decentralized and therefore immutable. This highlights the likelihood of heightened competition - probably assumed by the European legislator[1158] - between open and closed blockchains, as seems to be confirmed by the bundle of political and legal findings in the other European Regulations mentioned.

2.2 The legal challenges of identity 3.0: towards enhanced online rights

Decentralized digital identity brings with it legal challenges. The enhanced online rights it enables are numerous, including greater autonomy for users, better protection of privacy and reduced dependence on centralized trusted third parties. The legal stakes are therefore high, but require cooperation and regulatory alignment at national and international level. In concrete terms, by offering a strong, secure digital identity, decentralized identity can help strengthen people's rights, by giving them a means of proving their identity and protecting their personal data. Thanks to its online or offline accessibility, the attributes of an IND could also help combat discrimination and inequality by providing access to services for populations that are often excluded from them. In other words, every user becomes more autonomous, free and confident when it comes to online proof of identification and authentication. In principle, no unauthorized third party can thwart or prevent the user from identifying himself or herself to a digital service (public or private). Users' rights are thus "augmented" or rather "reinforced". The use of the term augmented in this study is intended to arouse immediate interest among the general public, given the many advantages of decentralized identity. No reference is made to a transhumanist meaning. The decentralization movement and technologies will enable people to

[1156] V. Appendices 3 & 6 & 7

[1157] Recital (9), "Building on the 'high' guarantee level, European digital identity portfolios should benefit from the potential offered by forgery-proof solutions", available at

[1158] Recital (35), "Certification as qualified trust service providers should provide legal certainty for use cases based on electronic registers. [...] Use cases involving crypto-assets should be compatible with all applicable financial rules, for example with the Markets in Financial Instruments Directive, the Payment Services Directive and the future Regulation on Crypto-Asset Markets [MiCA]".

This is only possible if legal and IT frameworks are defined to govern some of these forms of expression. While the massive use of decentralized identity attributes will probably take some time to spread in civil society due to its pre-industrial stage in 2023, the use of blockchain technology already has a notable head start for certain services, notably (crypto)financial. Thus, the gradual adoption of IND will mechanically imply a strengthening of the exercise of the rights of individuals and legal entities online, thanks to a new, more fluid, secure and interoperable digital identity. When a private or hybrid blockchain is used with IND standards, the level of confidentiality is strengthened, as user data is exchanged in a peer-to-peer, bilateral, selective and cryptographically verifiable way. These features are of particular interest for digital interactions between online public administration services and citizens wishing to carry out online procedures, whose data collection and processing by public authorities can be more transparent and better controlled, while being based on clear and unequivocal digital consent. This new 'cryptographic identity', which will in reality be computerized centrally, seems to perfect the concept of the '*networked citizen*' imagined in 2014 by Pierre Bellanger[1159] . However, decentralized identity may also have more nuanced implications in terms of intellectual property, liability, confidentiality and personal data protection. Users may indeed be tempted to falsify their digital identity or use the attributes of other Internet users for illegal purposes, raising issues of legal liability. The high level of confidentiality must not encourage fraudulent and illicit behavior, as can be the case today with certain messaging applications that are supposed to be end-to-end encrypted, such as Telegram or Signal[1160] . It is therefore up to IND's solution providers, as well as the legislator(s), to strike a balance between 3.0 technical innovation in data protection and the alteration of legal certainty it can engender in the case of anonymity in relation to illicit activities. National jurisdictions may also have different approaches to the regulation of decentralized identities, which can make it difficult to establish common standards. Despite these challenges, which seem rather limited to INAS, the advantages of a distributed digital identity outweigh its potential disadvantages. Finally, it's important to realize that in Web 3.0, regulators are almost as important as regulation itself. Indeed, if the regulators who interpret the regulations have sufficient knowledge to understand the stakes of what they are discussing, the legislative stances in response will have every chance of being computationally and socially pragmatic and proportionate.

[1159] BELLANGER Pierre, *La souveraineté numérique*, *op. cit,* in *Revue Le Débat* 2012/3 (n°170), pp149-159.
[1160] ROOSE Kevin, CHEN Brian, "Are Telegram and Signal the Next Misinformation Hot Spots?", February 30, 2021, in *The New York Time,* accessed online March 1, 2022.

2.2.1 Reinforced confidentiality of correspondence and business information

Correspondence and business secrecy are major concerns for individuals and companies alike. With the development of information and communication technologies, protecting the confidentiality and security of data and communications has become more complex. Respect for the secrecy of correspondence and business is an essential condition for the protection of individual freedoms and the economic interests of individuals and companies. On a national scale, Law n°2018-670 of July 30, 2018 on the protection of business secrecy, taken in application of European Directive (EU) 2016/943 of the European Parliament and of the Council of June 8, 2016, sets the legal framework for the protection of business secrets[1161] . Since 2018, the conditions of application have been strict without hindering the right to freedom of expression and communication, an employee's right to information, or the right to protection of a legitimate interest recognized in particular by European Union law[1162] . In practice, each situation is assessed on a case-by-case basis in the light of article L.151-1 of the French Commercial Code[1163] . The question of the proof to be provided is always complex, but verifiable certificates (VCs), mentioned in the previous chapter, can offer a new solution by enabling each person to prove the sending, receiving, sharing or accessing of information to or by a third party. Given that consent is essential for an IND, this enables a new form of cryptographic traceability that is difficult to contest, helping to reinforce people's rights. Distributed digital identity thus offers a source of online trust, as well as a form of presumption of reliability for correspondence, to which cryptographic evidence complying with data protection law is associated. Today, mostly linked to closed blockchains, an IND thus seems likely to guarantee the conditions for safeguarding the secrecy of correspondence and business secrecy, through the certain identification of information and its authors, in a probative, secure and resilient manner. Technological advances have opened the way to new IT solutions that reinforce the effectiveness of the law, by ensuring the confidentiality of exchanges and communications.

[1161] Loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, supplemented by décret n°2018-1126 du 11 décembre 2018 relatif à la protection du secret des affaires, pris en application de la Directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secret d'affaires) contre l'obtention, l'utilisation et la divulgation illicites.

[1162] MORALES Valérie, " Mais le secret des affaires n'est pas un talisman absolu ", in *Marvellavocats.com*, Les actualités de Marvell Avocats, see also De MAISON ROUGE Olivier, avocat, " Petit guide juridique de protection du secret des affaires ", 1ère parution, 13 octobre 2020, in *Village de la Justice*.

[1163] Art. L.151-1 of the French Commercial Code "Any information meeting the following criteria is protected as business information: 1° It is not, in itself or in the exact configuration and assembly of its elements, generally known or easily accessible to persons familiar with this type of information by virtue of their activity; 2° It has an actual or potential commercial value because of its secret nature; 3° It is the subject of reasonable protective measures by its legitimate holder, given the circumstances, to preserve its secret nature".

2.2.2 Simplifying and strengthening contracting

Without repeating the conditions for the conclusion of a contract, as set out in articles 1112 to 1127-6 of the French Civil Code, nor the provisions of law no. 2000-230 of March 13, 2000[1164] on electronic signatures, which is over twenty years old, dematerialized exchanges have since developed considerably. It is trust between contracting parties that ensures the proper execution of a contract over time. It is therefore essential for contracting parties to be able to identify themselves from the outset, to exchange information with certainty, and to verify the quality of the personal or contextual information exchanged. Distributed digital identity standards provide this guarantee through the reception, assimilation and consent of the parties via 3.0 attributes (VC, DID). In this respect, these cryptographic standards, which are in the process of being legally recognized, are useful for deeds signed under private signature, which account for over 90% of citizens' written documents[1165] . This study thus suggests that DID is a technological innovation that can simplify and strengthen online contracting. Thanks to these technologies, contracting parties can exchange confidential and secure information without the need for intermediaries to validate their identity. This reduces the costs and time involved in verifying identities, which can also speed up the conclusion or amendment of contracts. What's more, distributed identity guarantees the authenticity and integrity of information exchanged between parties, ultimately enhancing the trust and credibility of online transactions. By gradually incorporating these new 3.0 technological building blocks, contracting parties can benefit from a tailored and more efficient legal framework for the conclusion of phygital contracts, which would seem to favor the development of the digital economy. Distributed identity strengthens both the theoretical framework of contractualization (ex post and ex ante) and its final execution. From the identification of parties to the legal quality of exchanges and/or the archiving of information (documents, mandates, beneficiaries), the contractual relationship can be enhanced, i.e. strengthened to achieve a new form of legal optimization.

2.2.3 Towards greater consent for Internet users

Consent can be defined as the will to commit one's person or property, either tacitly (assumed) or expressly (expressed)[1166] . A person's consent can be deduced from a set of apparent and unequivocal elements. However, in 2020, the CJEU ruled that passive or tacit agreement online does not necessarily imply consent, in particular "*in the case of*

[1164] Law n°2000-230 of March 13, 2000 adapting the law of evidence to information technologies and relating to electronic signatures, JORF of March 14, 2000.
[1165] OUCHALLAL Mehdi, "Acte sous seing privé: de quoi s'agit-il?", in *LegalPlace,* 2022, available online
[1166] BRAUDO Serge, Honorary Advisor to the Versailles Court of Appeal, "Definition of consent", in *Dictionnaire de droit privé*, available online.

silence, default checkboxes or inactivity"[1167] . Indeed, the formation of a clear and unequivocal will in terms of online consent often seems incomplete when reduced to a few clicks of the keyboard or mouse on an online service. Some digital consents thus meet only part of the transparency criteria set out in article L.111-1 of the French Consumer Code, which stipulates that "(...) *the professional communicates to the consumer, in a legible and comprehensible manner, the following information: 1° The essential characteristics of the good or service, as well as those of the digital service or digital content, taking into account their nature and the communication medium used, and in particular the functionalities, compatibility and interoperability of the good comprising digital elements, the digital content or the digital service* (...)"[1168] . As a result, many online services struggle to ensure that the contractual conditions associated with their digital services are sufficiently clear and comprehensible to their users, in terms of consent[1169] . Indeed, every Internet user could regularly question his or her consent and associated actions, due to certain (pre)contractual information that is often insufficient or even unintelligible. Online consent should ideally be the result of personal activity, to rule out any random interpretation. This presupposes full information and understanding of the rights and obligations associated with each online service. To this end, the tools and intrinsic qualities of the IND seem relevant. Because the notion of consent is based on the digital transparency of the goods or services in question, as demonstrated above in its technical aspects, it offers, by design, a high degree of traceability and IT transparency. The IND thus contributes to reinforcing, i.e. optimizing and increasing, a person's online capacity to consent. In this sense, consumer law rules and IND IT standards seem to complement each other in their respective IT and legal techniques, to the benefit of individuals and their online identities. For example, since 2021, IN Groupe, Orange and Agdatahub have been offering a distributed digital identity solution called "*Agriconsent*". This 3.0 solution, which articulates INDs with a private blockchain, works - via a PIND - to serve an unprecedented consent for the 80,000 farmers listed in France. Decentralized identity is proving to be particularly relevant in terms of information. Article L.1112-1 of the French Consumer Code stipulates that "*any party who is aware of information whose importance is decisive for the consent of the other party must inform the latter of this fact if, legitimately, the latter is unaware of this information or trusts his co-contractor.* (...) *It is incumbent on the party who claims that information was due to him to prove that the other party owed it to him, it being incumbent on this other party to prove that he provided it*"[1170] . The laws on

[1167] CJEU ruling, November 11, 2020, Case C-61/19 Orange Romania SA v. Romanian National Authority for the Supervision of Personal Data Processing, in the context of a question referred to the Court for a preliminary ruling.
[1168] Art. L.111-1 of the French Consumer Code in the version in force since October 1er 2021, Livre Ier : Informations des consommateurs et pratiques commerciales - Légifrance, consulted online February 16 2022.
[1169] SOLANS Julia, "Succeeding in reading the SNCF's CGU will take you nearly 7 hours!", February 4, 2022, in *Capital.fr*
[1170] Art. 1112-1 of the French Consumer Code in the version in force since October 1er 2016.

Personal data laws systematically provide for legal processing based on consent, as well as a number of exceptions where consent is not required. For example, it must be possible to revoke consent in the case of recurring digital relationships. In healthcare law, consent is the free and informed agreement of a natural person to receive medical treatment or care. Consent must be given voluntarily and cannot be obtained by force, violence (harassment), threat, coercion, manipulation, intimidation, fraud or breach of trust. These offences are now being transposed and observed online, sometimes to the point of physically affecting Internet users. Health law therefore requires informed consent, which means that the individual must have sufficient information on his or her state of health, on the medical treatment or care proposed to him or her, with the potential risks and benefits, as well as on the possible alternatives available to him or her. In this respect, the person must have the time and opportunity to ask questions and receive answers before giving consent. According to this study, these provisions of the French Public Health Code[1171] could inspire legislators to strengthen the online consent of individuals, which is currently insufficient in view of ongoing online exchanges. While tacit consent may sometimes suffice, the significant scope of the IND as a reliable IT tool ensures effective consent in the service of citizens' daily online and offline lives. This notion of cryptographic consent is at the heart of this 3.0 identity, and the DIF[1172] , mentioned earlier, is already proposing the standardization of 3.0 consent receipts (referred to as "*Data Agreement*")[1173] for the storage and traceability of digital consents (VC).

2.2.4 Greater online freedom of expression for citizens

Freedom of expression is a fundamental right enshrined in the French Constitution and recognized by numerous international treaties and conventions. It is the right to express oneself freely, without censorship or restriction, whether in writing, orally or by any other means of communication. A person's identity is intimately linked to their freedom to express themselves, to think and to choose, in other words, to their ability to assert all or part of their identity. Freedom of expression can therefore be understood from an identity angle, through the different ways in which it can be exercised online, in other words, through one's lived identity. It thus represents the right to choose the medium

[1171] Art. L1111-2 Code de la santé publique: "Toute personne a le droit d'être informée sur son état de santé [numérique]"; Art. L1111-4 Code de la santé publique: "Toute personne a le droit de refuser ou de ne pas recevoir un traitement [informatique]" (here added and underlined by the author).
[1172] "The Decentralized Identity Foundation (DIF) exists to advance the interests of the decentralized identity community (...) ", in *Identity.foundation.com*.
[1173] These consent receipts are aligned with ISO standards, and some companies are about to launch a new project as part of the *Decentralized Identity Foundation,* notably to define the reference protocol and implementation for these "Data Agreements".

to express themselves. The Conseil d'Etat points out that freedom of expression occupies an essential place in the system of fundamental rights. As a condition of freedom of thought, it expresses the identity and intellectual autonomy of individuals, and conditions their relations with other individuals and with society[1174] . A close link between freedom of expression and freedom of informational self-determination[1175] is thus emerging, to the benefit of personal identity and this fundamental right. Self-sovereign digital identity (INAS) thus seems to come close to the perception and desire for total freedom of expression mentioned by French philosopher and humanist Simone Weil in 1949: "(...) *total, unlimited freedom of expression, for any opinion whatsoever, without any restriction or reservation, is an absolute need for intelligence*"[1176] . It is therefore up to the State to ensure, at all costs, the possibility of freedom of expression online, by guaranteeing its role as a builder of expression and public debate, while certifying the reliability of the IND solutions available to users (in line with eIDAS-2 mentioned above). As far as self-sovereign digital identity solutions are concerned, it's important not to try to ban them or hinder their development, which is already limited by the market, as demonstrated in this study. Finally, Web 3.0 could offer innovative technological means to reinforce this universal right to expression, or at least contribute to it. Citizens can therefore avail themselves of online freedom of expression, within the limits of positive law, which can limit its scope and expression in certain legitimate cases, where 3.0 tools would become as much mechanisms for defending as for controlling this universally-applicable right.

2.2.5 Towards informational self-determination of personal identity

It should be remembered that the growing availability of personal data on computer networks, with their multiple applications, tends to diminish the importance of controlling one's data, while blurring the essential notions of consent and free will. Throughout history, many individuals have privileged one or more facets of their identity to the detriment of others (censorship, information control). This observation, which seems to have been repeated since the advent of the Internet, highlights a new legal trend in favor of the introduction of an old principle from German law, the right of individuals to "*informational self-determination*"[1177] . This trend has its origins in a ruling of December 15, 1983

[1174] VERPEAUX Michel, "La liberté d'expression dans les jurisprudences constitutionnelles", 2022, in *Conseil constitutionnel*, available at the following address
[1175] See next section.
[1176] WEIL Simone, "L'enracinement: prélude à une déclaration des devoirs envers l'être humain", 1949, coll. idées, available at
[1177] Translated from the German "Selbstbestimmungsrecht". This term can be translated as "right to self-determination" or "right to personal self-determination".

of the German Constitutional Court ("*Karlsruhe"*)[1178] . In German law, this concept is often used to refer to a person's fundamental right to make decisions about his or her own life, to exercise a degree of freedom and autonomy in his or her choices, and to be protected from unwarranted interference by third parties or the state. Article 2 of this law guarantees everyone's right to personal freedom, which includes the right to self-determination[1179] . This right is often invoked in contexts such as the right to privacy, the right to physical and psychological integrity, the right to choose one's place of residence, the right to decide one's own sexual orientation or gender identity. Finally, this right is an important concept in German law, which protects the fundamental right of every person to make autonomous decisions about his or her own life, provided that these decisions do not interfere with the rights and freedoms of other people, or with the public interest. Applied to the digital sphere, this right thus advocates the individual's ability to control his or her personal data[1180] . As Aurélien Bamdé, Doctor of Law, reminds us, the Court "[German Constitutional Court] *guarantees in principle the individual's ability to decide on the communication and use of his or her personal data [...] self-determination is an elementary functional condition in a free democratic society, based on citizens' ability to act and cooperate*"[1181] . Informational self-determination therefore consists in enabling individuals to control the collection, use and sharing of their personal information, by giving them the opportunity to choose whether or not to share it, to access it and to correct it if necessary. This becomes particularly important in today's digital environment, where personal data can be easily collected and stored. This approach seems to protect the privacy and autonomy of each individual by ensuring that organizations collecting personal information are transparent about how it is used, and do not use it for purposes other than those for which it was collected. Although identity is both inclusive and exclusive[1182] , informational self-determination aims for a more inclusive identity. This approach is linked to the digital identity of individuals and could be explicitly recognized within the EU to better protect personal data. However, this study asserts that the physical existence of each individual must always be superior to his or her digital representation, contrary to some of the utopian promises of Metavers, which is explored below. Informational self-determination could

[1178] The Federal Constitutional Court is the supreme judicial body for constitutional matters in Germany. It is responsible for ensuring compliance with the German Constitution, the Basic Law, and for protecting the fundamental rights of German citizens. The term "*Karlsruhe" is* often used to refer to the Federal Constitutional Court itself, or to its decisions, which often have a significant impact on German political and legal life.
[1179] Art. 2, [Freedom to act, freedom of the person] (1) "Everyone has the right to the free development of his personality provided he does not violate the rights of others or infringe the constitutional order or the moral law", available at
[1180] BAMDE Aurélien, "Informational self-determination", §2: The right to informational self-determination, 2018, in. *aurelienbamde.com*, consulted online February 9, 2022.
[1181] *Ibid.*
[1182] *Op. cit,* MAALOUF Amin, "Les identités meurtrières", "[...] thanks to each of my belongings, taken separately, I have a certain kinship with a large number of my fellow human beings", p.27.

contribute to the data minimization and consent requirements mentioned above[1183] , thanks to digital identity solutions (IND), provided that these solutions are governed by European regulations such as eIDAS-2. In order to adopt such a system, it would be wise for everyone to take a "digital *identity test*"[1184] beforehand, so as to become conceptually aware of their online identity, while avoiding certain well-known abuses. Finally, access to government services without digital identification must be maintained in favor of the possibility of physical identification or reliable digital delegation systems. Finally, the right to data protection is often seen as a defensive measure, whereas the right to informational self-determination proposes a more proactive approach, as it is aligned with European texts dedicated to data protection and based on the values of the individual. This ambitious approach aims to restore individuals' control over their personal data, which is gradually being perceived and treated as a commodity to be traded[1185] .

2.2.6 The reinforced utopia of patrimonialization and property rights over data

The notion of property in its general acceptation is expressed through the goods a person possesses, these being in reality only an extension of the full personal and claimed ownership of a person in relation to others. Property is thus an extension of our most personal identity, that is, of ourselves, as defended by John Locke[1186] . For example, owning a house provides a sense of security and confidence, as it enables the owner to demand the departure of anyone who enters his home without his consent, without any subjective link to the property in question. Consequently, the right of ownership creates a relationship of power and domination. However, this preliminary reasoning seems to apply above all to primary (and not secondary) identity data[1187] . The right of ownership over a thing can only endure over time thanks to a legal and root identity administered and made possible by a state governed by the rule of law. Nevertheless, it seems important to distinguish between our identity and the property we acquire, in order to address the issue of the commercialization of personal data. While the boundary between the two may be narrow and ductile, it is nonetheless crucial, since an identity attribute emanates from our own existence, unlike an acquired good. It must therefore be borne in mind that a datum is not a tangible good - quite the contrary. Faced with the reproduction dilemma

[1183] SCHWAB Pierre-Nicolas, "Statistiques RGPD Europe : évolution du nombre de plaintes par pays", "64% of English DPOs have seen [2018] an increase in the number of requests after the implementation of the RGPD", 2019, in *intotheminds.com*, accessed online February 9, 2022.
[1184] MAALOUF Amin, "Les identités meurtrières", p.23.
[1185] See next section.
[1186] BREMAEKER Nathalie, "L'identité de la personne humaine au croisement du droit et de la psychanalyse", Thesis in Law at the University of Perpignan, 2021, "John Locke was already defending the idea that we are owners not only of our property but also of ourselves", p.274.
[1187] V*, supra*, I, Title 1, 2.2

[1188] , decentralized technologies hold out the promise of a new Holy Grail of digital ownership. As author Pierre Bellanger points out[1189] , data no longer belongs to users, although some of the most decentralized crypto-assets do not[1190] . In theory, these new IT and business models could offer users of online services the possibility of receiving partial or total remuneration in crypto-assets in exchange for sharing their digital identity attributes, either through the sale of their personal data. The aim of data patrimonialization is therefore not only to create passive income for Internet users (commercial and advertising aspect), but above all and supposedly to reintegrate this individual value into a collective value chain where the physical person, issuer and source of data, once again becomes the central and essential actor of his or her identity. In Pierre Bellanger's view, it's a question of recognizing that the root of the problems linked to data stems from a failure to recognize their right of ownership. In his view, we simply need to "(...) *extend the status of personal data to the entirety of a person's computer trace, and recognize it as intangible property*"[1191] . Theoretically, such a legal reappropriation would enable individuals to freely delimit the use they make of these intangible assets, in exchange, for example, for a ban on their use or transfer to third parties. Intangible property is property that does not have a physical or material form, but does have an economic value. They include items such as intellectual property rights, trademarks, patents, licenses, know-how, databases, trade secrets and other economic benefits they represent. Legislators and public institutions have approached the issue of personal data from a utilitarian angle, with the aim of protecting individuals' online rights. To this end, a classification and jurisprudential nomenclature have been established, with several categories of data (health data, religious data), in order to regulate the use of each type of data and prevent abuse. However, this nomenclature excludes certain types of data from its protection, such as certain professional data that are not necessarily considered personal or sensitive data within the meaning of this nomenclature, a loophole identified and enshrined in the section dedicated to the RGPD[1192] . In 2022, legal discussions focus on privacy protection rather than property rights, which are still considered a complex subject by legal experts.

[1188] PERRY BARLOW John, "If our property can be infinitely reproduced and instantly distributed around the planet at no cost, without our knowledge, without it even leaving our possession, how can we protect it?", 1994, in *The Economy of Ideas*, consulted online at wired.com

[1189] "*Res nullius*" is a Latin expression used in civil law to designate a thing without a master, i.e. one that has no owner but is nevertheless appropriable. BELLANGER Pierre, "La Souveraineté Numérique", *op. cit,* "To this day, data does not belong to anyone in law. They are res nullius.

[1190] See related section *above*

[1191] *Op. cit,* BELLANGER Pierre, "La Souveraineté Numérique", Ed. Kindle, location 2569 of 3565.

[1192] See *supra*, I, Title 2, 2.4.

This reluctance to recognize a patrimonial right to personal data was highlighted as early as 2014 by the Conseil d'Etat[1193] . In this 2014 study, the Conseil d'Etat ruled that it was not desirable to transform the subjective right to protection of personal data into a patrimonial right. It is therefore necessary to take into account the complexity of this issue in an attempt to provide elements of a response from both a legal and IT perspective. According to Gaspard Koenig[1194] , a French essayist and philosopher, it is clear that online data is being abandoned in favor of free, permanent access to online services. According to this author, this opaque cession without equivalent consideration of the emanation of our "*self*" - non-corporeal in his view - is possible under cover of an illusion of online data protection fueled by the RGPD. Gaspard Koenig points out that this oligopolistic management of data would be comparable to a "*feudal digital system*"[1195] . Since data has value, why not simply recognize it? How much is data worth, and is this digital object worth it?[1196] Faced with this unprecedented centralization of people's data within a seemingly infinite digital sphere, two main currents of thought are clashing in terms of data valuation, the first (i) against a monetization or patrimonialization of personal data, and the second (ii) in favor of such a principle.

(i) Some legal experts and institutions (CNIL) believe that the RGPD offers adequate guarantees to deal with the massive collection of data generated by individuals[1197] . Moreover, some consider that monetizing data does not confer a right of ownership over it, suggesting that an intermediate boundary would exist between data protection and monetization. In reality, it seems that these data monetization contracts do not constitute a "*sale*"[1198] of personal data, but rather an authorization to exploit it in compliance with the aforementioned legal framework. In France, the unavailability of civil status data, as well as federated and regalian digital identity solutions such as FranceConnect, ensure a definition as well as a form of protection of people's rights to carry out certain online interactions. On the other hand, common law in the United States allows the transfer for consideration of

[1193] Sénat, "Projet de loi pour une République numérique", Rapport n°534 déposé le 6 avril 2016, in www.senat.fr, consulted online on November 20, 2021, "the Conseil d'État, in its 2014 study, considered that it was not desirable to transform the personal right to protection of personal data into a patrimonial right.".
[1194] KOENIG Gaspard, "[...] the self has never been so much in demand. It's time to understand to whom it belongs", "La propriété de soi", accessed online on November 18, 2021.
[1195] A parallel can be drawn with the Middle Ages, when peasants provided their lords with all or part of their harvest in exchange for protection against enemy attacks. In a similar way, Internet users cede all or part of their online data (often via opaque, unintelligible or even leonine GTCs) in exchange for free online services.
[1196] According to the online simulator simulator.drdata.io, the value of the personal data of the author of the present research is worth around 109 euros in 2022. According to this simulator, it is noted that the *primary identity data* that appear to be most financially valued are the level of education, the social security number and the telephone number, which are worth more than other *data* identified as *secondary* by our study (see the "CSP" and "Internet & Consumption" categories).
[1197] ANCIAUX Arnaud, FARCHY Joëlle, "Données personnelles et droit de propriété", in *Rev. Int. Droit Econ*, 2015, accessed online on November 20, 2021.
[1198] "Annales des Mines N°18 sur les Enjeux Numériques: Propriété et gouvernance du numérique", *op. cit.* p. 30.

certain parts of the human body[1199] , which, by ideological extension, opens the door to the patrimonialization of personal data, whether considered tangible or intangible. In our positive law, such a position would contravene the principle of data unavailability, a boundary already adopted in most countries around the world. Because data characterizes a person, it seems that it must remain unavailable to any third party, just as the human body cannot be commercialized under domestic law.

(ii) Some thinkers believe that recognizing data as heritage would enable a new emancipation of data and its exchange. This position is based in part on John Locke's postulate that each individual possesses a property in his or her own person, which no one else can claim[1200] . To achieve this recognition, a number of contractual mechanisms could be envisaged, such as the extension of property rights to personal data, or licensing, rather than the social and temporary ownership proposed by Thomas Piketty, economist and Professor at the EHESS[1201] . According to Gaspard Koenig, the absence of self-ownership is a theological vestige in our law and social organization that prevents us from determining our own values[1202] . The main challenge of this financial recognition of our digital heritage is not only technological, but above all moral and political. We need to ask ourselves whether valuing people's data and their identity is beneficial, and whether we are prepared to abandon our democratic conception of autonomous judgment in favor of foreign entities, or whether we are going to reclaim our data in the name of a digital society liberated thanks to Web 3.0. It is also pertinent to ask why the monetization of our data would be unavailable, or even prohibited, when paradoxically many online services implement it through subtle legal arrangements such as the application of general conditions of use (CGU) or digital adhesion contracts, from which Internet users cannot escape within Web 2.0. A right of ownership over our personal data would enable us to dispose of it freely (sharing, transfer, destruction) in accordance with the provisions of article 544 of the French Civil Code, which states that

[1199] KOENIG Gaspard, "La propriété de soi", *op. cit*, "[...] certain parts of the body such as hair, or blood in the United States, can be objects of commerce", p.2.
[1200] LOCKE John, "Second Treatise, § 25--51, 123--26. Chap. V. of Property," accessed online November 20, 2021, "each Man individually possesses a property on his own person; it is something that no one else has any right on it", in *Report* "Mes data sont à moi. Pour une patrimonialité des données personnelles", LANDREAU Isabelle, PELIKS Gérard, BINCTIN Nicolas, PEZ-PERARD Virginie et al, 2018, available at, p.18.
[1201] PIKETTY Thomas, "Je propose de dépasser la propriété privée par la propriété sociale et temporaire", accessed online November 20, 2021, September 9, 2019, in *France Inter*, available at.
[1202] KOENIG Gaspard, "La propriété de soi", *op. cit*, "L'absence de patrimonialité de soi empêche nous de déterminer pour nous-mêmes nos propres valeurs. It is a theological remnant in our law and social organization".

"property is the right to enjoy and dispose of things in the most absolute manner (...)
". However, the right of patrimoniality over such data depends on free will and prior capacity, i.e. being free to choose to dispose of oneself. Because the right of ownership is a real right ("*Ius in re"*) that relates to a thing, it would be necessary to qualify personal data as intangible and real property, as mentioned above. In this configuration, a person's right to dispose of his or her data would in practice end where the right to dispose of another person's data begins:

a. The 1978 law (CNIL) supplemented by the RGPD Regulation, which establishes strict rules for protecting people's privacy. Personal data may not be collected, used or communicated for commercial purposes without the prior and informed consent of the persons concerned. Once such consent has been recorded, partial monetization of data is possible within the contractual limits imposed by these Regulations (framed harvesting, right of withdrawal, deletion of data, etc.).

b. The point is to understand whether the right would treat all existing intangible property (such as personal data) equally, and whether the owners of such property could benefit from it in a similar way. However, in certain situations, the creation of derived or aggregated data could undermine the substance of the original data (its root and pivot attribute), thus altering the property right by underlying effect. The systematic contractualization of exchanges concerning personal data, thanks to decentralized identity, would imply that the identity of individuals would be subject to this contractualization. However, property rights would allow everyone to freely choose their values, whether positive or negative for the common good.

c. The right to dispose of and perform all acts likely to lead to the voluntary total or partial loss of one's intangible property, the owner being vested with the power to affect the substance of the thing by certain material acts (consuming it, destroying it, improving it) or legal acts (transferring it, dismembering it).

The following table summarizes the arguments for and against the patrimonialization of data:

Arguments FOR	Arguments AGAINST
The patrimonialization of Internet users' data, subject to specific contractual conditions such as the duration and type of data concerned, enables them to be valued via purchase and sale transactions. This could help to raise awareness among individuals of the value of their personal data, and even make them more responsible for it.	In legal terms, there is a risk of conflict of laws, as far as the transfer of personal data is concerned. Some legal experts consider that this practice is contrary to the public order provisions of the 1978 Data Protection Act and the RGPD Regulation, which compromise both the monetization of data. To recognize a right of ownership over one's data, it is necessary to answer certain questions and uncertainties, such as how to identify with certainty the owner of a piece of data, or how to manage conflicts of law between strict data protection regimes (RGPD in Europe) and those likely to accept a patrimonialization of data as in the United States. Implementing a monetization of personal data is possible, but implies a restrictive legal framework[1203] and in reality very often utopian for end users, as some legal experts suggest: "*for the legal expert, it is clear that the RGPD does not facilitate the implementation of monetization. Moreover, beyond the legal issues, monetization is often a fool's bargain for the data subject, either because he or she is not really aware of this monetization, or because he or she has no real choice if he or she wants to benefit from a service, or finally because he or she only derives a minor economic interest when he or she decides to market, himself or herself, his or her data*"[1204] .
Subject to the use of 3.0, the patrimonialization of data would make it possible to ensure computer security and cryptographic control of data by individuals, thus theoretically reducing the unauthorized use of their personal data.	From an IT point of view, there is a risk of a "*honeypot* effect"[1205] , i.e. a phenomenon that attracts hackers. The more valuable and grouped (centralized) the data, the greater the risk of it being attacked and plundered, hence the importance of distributing/decentralizing it.
Blockchain technology and decentralized identity could dispel the economically non-rival nature of data that currently prevents its patrimonialization. In other words, these technologies	From an economic point of view, data is considered to be a non-rival good, i.e. it can be used by several people simultaneously or not, unlike a rival good whose consumption by one person prevents consumption by another (due to the phenomena of cryptographic uniqueness and scarcity). This

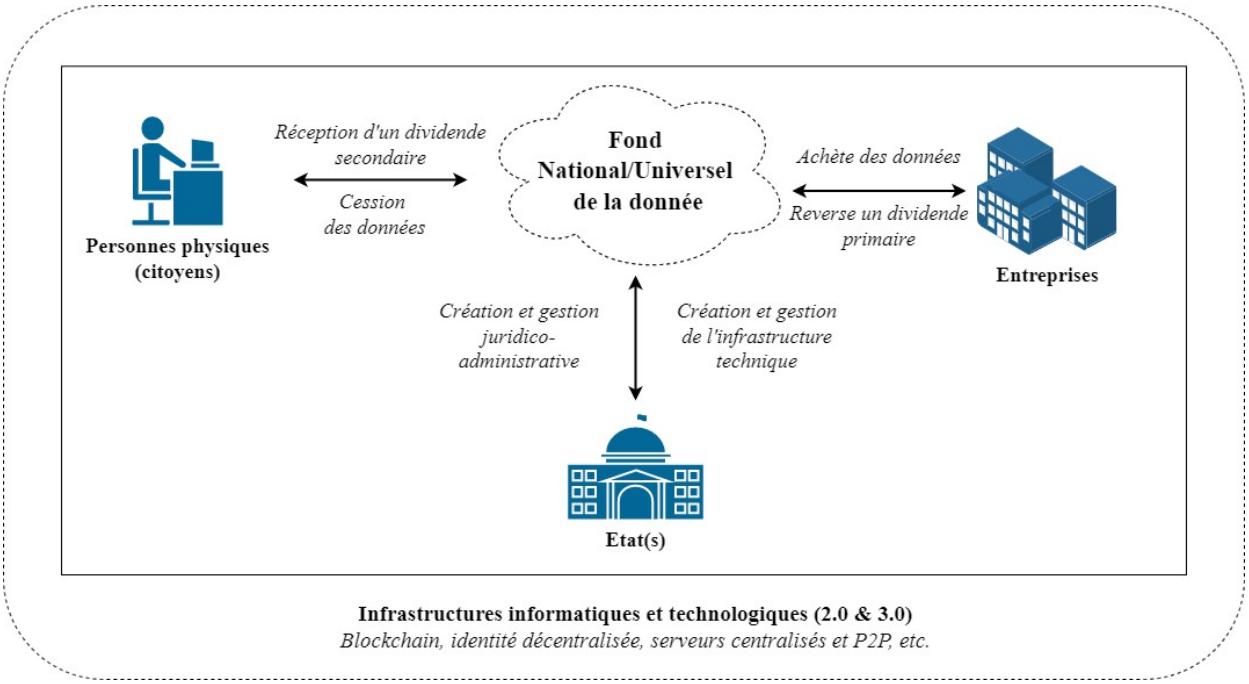
[1203] "Annales des Mines N°18 sur les Enjeux Numériques : Propriété et gouvernance du numérique", *op. cit.* pp.30-31.
[1204] *Ibid*. p.32.
[1205] As a reminder, the centralization of data by one or a few identified entities can have the effect and tendency of attracting the covetousness of hackers, whose search for ill-gotten gains can be facilitated, which supports the use of truly decentralized and resilient IT systems.

will allow for the first time that the consumption of data by an online service is exclusive, a concept that until now has not been very effective with digital identity 2.0.	This characteristic is explained by the possibility of duplicating data on the Internet, as previously studied[1206] .
Patrimonialization represents an extension of the right to informational self-determination we have outlined, and would help to reinforce or even institute it. In this respect, in China and Russia, data is often regarded as a common good, belonging to the community (*see* below). This approach aims to prevent scandals linked to personal data breaches by adopting a more collective perspective for the management of such data, in terms of scope and/or extent.	Recognizing a right of ownership over personal data contravenes the principle of the unavailability of a person's civil identity[1207] . Indeed, granting individuals a right of ownership over their personal data would be tantamount to conferring on them an availability over their data and, by extension, their digital identity, whereas such data should not, in principle, be subject to availability, in particular to avoid any attempt at patrimonialization without their knowledge (non-consensual commercialization, identity theft, manipulation).
	In France, property rights apply to movable or immovable objects, which poses a problem when the object in question is data, which is fluid and non-static by nature. In fact, the constantly evolving state of this data may require the application of various legal regimes, simultaneously or not, depending on the context of use (financial, professional, personal), making its legal protection complex. For example, according to the Association francophone des autorités de protection des données personnelles (AFAPDP), founded in 2007, personal data are an integral part of the individual and their rights are inalienable, meaning that they cannot be sold or transferred to third parties[1208] . In this respect, personal data is inseparable from the data subject and cannot be separated for transfer to a third party.

In 2019, private law professor Valérie-Laure Benabou of the University of Versailles Saint-Quentin-en-Yvelines (Paris-Saclay) proposed an alternative patrimonialization solution called "[1209] . This solution implies the creation of a national public fund for certain citizens' personal data. The management and intellectual property of this fund would constitute a national digital commons. This collective, rather than individual, approach to data patrimonialization recognizes the patrimonial nature of data while proposing

[1206] V*, supra,* I, Title 1, 2.3.1
[1207] See *supra,* I, Title 1, 1.1.3.
[1208] Vienumerique.ch, "Digital Integrity of the human person: A new fundamental right", 2020, [Slides], accessed online 15/01/2022, "Personal data are constituent elements of the person. Rights to personal data are inalienable, and cannot be sold", p.9.
[1209] Proposals from the AFDIT conference held face-to-face on December 6, 2019 in Marseille.

a common framework that transcends individual interests. The State would be the guarantor of this digital and informational commons, which would provide for the introduction of a "*data dividend*" levied by the State in return for the sale of certain data from the commons to online services. Note that the Data Act[1210] , due to come into force in September 2023[1211] , defines the notion of "*data altruism*"[1212] , which corresponds to the principle of this universal data fund. The latter could be used to establish a primary dividend for the benefit of the State, which would then be paid back to social and environmental causes, as well as a secondary dividend for the exclusive and free benefit of the people whose data has been used. However, no details have been provided as to the nature of the data included in this fund. With such a proposal enabling a first form of property right over such data, it would be possible to meet the interests of all parties involved: governments could levy taxes, online services could reap the benefits, and citizens/consumers could obtain compensation for the use of some of their data. To facilitate the implementation of this right, the use of technologies
3.0 could be advantageous, as it would facilitate the identification and traceability of the data concerned, thus reducing any lack of transparency. The following illustration provides a non-exhaustive summary of the elements mentioned, i.e. the overall operation that such a universal or national personal data fund could entail:



[1210] See *above*, I, Title 1, 2.2.1.
[1211] CNIL, "European strategy for data: the CNIL and its counterparts comment on the Data Governance Act and the Data Act "2022, available at
[1212] Art. 2 recital (16) of Regulation (EU) 2022/868 of the European Parliament and of the Council of May 30, 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation).

It's important to remember that self-sovereign digital identity (INAS) allows users' personal data to be stored only on their own hardware (phones, computers), and only selectively shared as proof of information. In addition, other 2.0 and 3.0 standards and applications, such as P2P servers, blockchains of all kinds, DAOs and zero-knowledge proofs (ZKP)[1213] discussed in the next section, provide suitable tools and foundations for implementing the previous illustration. It is possible to establish a virtuous economy by adopting the model of the cooperative society of collective interest (mentioned in the section dedicated to Kleros)[1214] , which would benefit all stakeholders in terms of governance (voting rights), whether they are natural persons or legal entities. However, for this model to be effective, it is necessary for the national data fund to be partially decentralized, which might not be accepted by the State due to its regal prerogative in this area, or due to the political difficulties studied throughout this research. Nevertheless, it seems that the State must remain the guarantor of such a system, having partial control over it, but above all total transparency. This would probably involve the use of distributed identity systems, or even self-sovereign digital identities (INAS), so that users can voluntarily feed the fund with their data. Finally, considering a partial recognition of a property right over data, it seems preferable to adopt a nuanced legal regime rather than simply applying the classic property right legal regime to personal data. A distinction needs to be made between use cases and types of data, particularly in the case of health, biometric or political data, for which data ownership cannot be applied without precaution. Finally, the patrimonialization of data could contradict several major Internet principles, such as the free circulation of public data, and move personal data from a collective and public stage to a strictly private and subjective one. It therefore doesn't seem necessary to turn data into property that can be bought and sold. Personal data is simply information about a person, and cannot be considered a commodity in the same way as a physical object. It is therefore more important to ensure that personal data is protected by adequate laws and regulations than to seek to patrimonialize it at all costs. If an extension of property rights to data is envisaged, it should at the very least be accompanied by secure and reliable technologies such as IND, ZKP and blockchain technology (probably private or hybrid). What's more, this extension should only be possible if citizens and Internet users give their free and informed consent, and if identity attributes can be revoked at any time by the interested party. In short, if such a desire for data patrimonialization were envisaged in the future, it would have to respect these conditions to be justifiable and lead, at most, to the type of concept summarized schematically in this section.

[1213] V. *infra*, II, Title 1, 2.2.6.1
[1214] See *supra*, I, Title 2, 2.7.2.

2.2.6.1 ZKP as a new reference tool for data protection

In June 2022, the CNIL laboratory announced the availability of an open-source demonstrator that uses a new cryptographic method called *Zero Knowledge Proof* (*"ZKP"*), an acronym we favor in this research[1215] . In this context, ZKP is an algorithmic concept that enables a holder to prove to a third party (verifier) that one of its proofs - of data - is authentic without revealing any information other than that required to prove the authenticity of said proof. In other words, ZKP enables a user to validate a transaction without disclosing his identity or, for example, the amounts of crypto-assets sent to another user. For the digital identity sector, ZKP can be used to cryptographically verify that a person is of legal age, without the verifier (police officer, restaurant owner, security guard) knowing the exact age - or other non-essential information - of the person being verified. The inspector simply knows that the person is over 18, which is sufficient information for the inspection to be carried out in full compliance. This technology thus makes it possible to respect user privacy in an unprecedented way, by minimizing the data transmitted to identity providers and online services. According to Gartner, ZKP technology is in an innovation phase and is expected to reach a "*productivity plateau*" in the next 2 to 5 years[1216] . The first practical implementation of this technological concept takes root with the "*zCash*" blockchain, which was launched at the end of 2016 using a variant of ZKP called "zkSNARK". This protocol(s) and technological concept allows multiple proofs to be generated and stored indefinitely on a blockchain, without each of them needing to interact with the verifier, enabling peer-to-peer (P2P) verification, respectful of personal data, by multiple third parties. Other protocols and blockchains, such as Hyperledger ("ZKAT") or Ethereum[1217] , are developing similar concepts of cryptographically programmed confidentiality. In the future, these 3.0 cryptographic bricks could be implemented on the Bitcoin blockchain, notably thanks to some of its new underlying protocols such as the "*Lightning Network*" and the "*Taro*" protocol[1218] studied in Appendix 6 (Focus 4). As a reminder, many identity providers collect more information than they need to verify an individual's identity. This massive collection of information, often for commercial rather than identification purposes, hinders the implementation of the principle of data minimization. The implementation of ZKP offers a structural solution to this problem, making it possible to provide irrefutable proof without disclosing its content. This cryptographic method represents an innovative technical tool for complying with the principle of personal data minimization dictated by the RGPD, but also reinforces the possibility of pseudo-anonymity through

[1215] GORIN Jérôme, BIERI Martin, BROCAS Côme, "Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée", 2022, in *linc.cnil.fr*, consulted on June 22, 2022, at the following address
[1216] V. Appendix 9.
[1217] V. Appendix 6, Focus 2.
[1218] V. Appendix 3, Focus 4.

online design. In addition, the ZKP can be applied in many fields, such as proof of diplomas[1219] , experience, training, legal acts, among others. ZKP would enable public or private organizations to prove their regulatory compliance without disclosing confidential information[1220] , in line with the already studied secrecy of business and private correspondence. Thanks to the concept and the various ZKP protocols being developed, many public, private or hybrid blockchains could comply with the aforementioned eIDAS, RGPD, MiCA or TFR regulations, provided their respective protocols allow this, i.e. by developing additional computing capabilities (second-layer or Layer 2 protocols)[1221] . Finally, ZKP coupled with a decentralized digital identity forms a powerful alloy at the service of a more data-friendly Web. The implementation of ZKP should therefore be supported by more IND solutions to guarantee optimal encryption and protection of individuals and corporate bodies in digital ecosystems 2.0 and 3.0.

2.2.7 The social potential and IT challenge of decentralized voting

The right to vote is essential to any democracy, as it guarantees citizens' freedom of expression within a state governed by the rule of law. As well as being a means of expression and governance for citizens, the right to vote symbolizes a counterweight to the established political order. Although its role is crucial, its implementation is complex to ensure democratic representation of society's expectations[1222] . Voting thus seems to be a tool for individual expression, rather than a guarantee of pure democracy. With the rise of online communication networks, the methods and forms of voting have expanded considerably, to the benefit of institutions and citizens alike. Today, every individual can express his or her opinion on countless subjects and in numerous contexts of varying degrees of significance and official status for society (professional votes, votes in elections, votes on social networks). These numerous contexts of digital expression calling on the votes of Internet users today make it complex to (i) identify and highly authenticate users during an online voting process, and (ii) ensure the authenticity (integrity, durability) of the votes cast. Thus, not all online votes require a high degree of authenticity.

[1219] Wikipedia, v. BCdiploma company, 2023, available at

[1220] More specifically, some public blockchains (*Monero*, *Zcash*) already use these advanced *ZKP* cryptographic processes. They enable crypto-asset transactions in which the participants' public keys as well as the transaction details are hidden from public view. While these blockchains are potentially more in line with the RGPD (since there is no longer any personal data visible), they do pose a major problem for the authorities in charge of combating money laundering and the financing of terrorism. The future therefore seems to lie in the hands of blockchains capable of reconciling the following imperatives: respect for their users' privacy and compliance with legal rules.

[1221] These second-layer systems can be directly ("*Layer 2"*) or indirectly ("*Sidechain"*) linked to the main blockchain and protocol, using more or less similar and complex IT modalities. In other words, a *Layer 2 relies* on the security of an existing blockchain network, while a *Sidechain* relies on its own IT security model.

[1222] MAALOUF Amin, "Les identités meurtrières", *op. cit*, "A vote merely reflects a society's vision of itself and its various components. It can help to diagnose, but it can never be the sole remedy", p.180.

expression and reliability. At present, it is accepted that two types of electronic voting coexist:

a. Mixed face-to-face voting, but with voting computers or "*voting machines*"[1223] . These special[1224] computers are used in some polling stations in France. These polling stations no longer require polling booths or ballot boxes to cast their votes, and citizens have no choice but to vote on these machines, which record and digitize all voters' results. To date, this solution remains very limited, due to complex logistics for local authorities and restricted accessibility for voters.

b. Remote digital voting, i.e. by digital correspondence, which is particularly effective in combating voter absenteeism (especially during the Covid-19 crisis). Although this type of voting is currently only possible and in force for French MPs abroad[1225] , these votes often have a national and official character, and are directly linked to the voter's civil identity. In other contexts (professional, academic, leisure), people cast votes with little legal impact, but sometimes with high personal added value. These low-level votes are carried out via a variety of 2.0 platforms that are more or less reliable, credible or official. These platforms generally collect personal data on their users, and for more or less legitimate reasons (in principle, to help them improve their operations, sometimes with a few deviations). For example, while current solutions enable the pseudo-anonymization of user data, it is often impossible for these platforms to prove to their users that their data is indeed pseudo-anonymized. Indeed, a user's vote could be disclosed to third parties via a virus hosted on the voter's computer or directly on the platform, and without the knowledge of either the vote host or the user. In such a case, the vote would be biased and null and void, and would have to be re-run (on the assumption that the computer intrusion is identified and not latent).

As a result, online voting 2.0 is associated with the issue of digital trust already mentioned above. The 2.0 trust granted to these platforms appears to be legal rather than cryptographic, as the platform can prove its IT solidity via state support.

[1223] Article L57-1 of the French Electoral Code, available at the following address
[1224] These voting computers are a model approved by the Ministry of the Interior, authorized by the Order of November 17, 2003 approving the technical regulations setting the conditions for approval of voting machines.
[1225] Service Public, "Vote d'un Français installé à l'étranger", 2022, in *servicespublic.fr*, consulted on 01/02/2022.

and institutional (guarantees, certifications)[1226] , but it cannot directly prove its cryptographic solidity to users, even though Web 3.0 and ZKP now make this possible. However, how can we be sure that a vote is computer-valid, and that it does indeed emanate from the voter's will and civil identity? While these problems are fairly limited for low-value votes, as we have seen (as they do not require the voter's civil identity), they remain essential for the official votes that underpin our democracy and rule of law. Citizens and Internet users are in favor of new online voting systems via official websites and uncomplicated identification and authentication systems. However, it seems that these 2.0 systems face numerous technical challenges that can only be solved with the addition of other 3.0 technological bricks such as blockchain technology and decentralized identity. It is therefore important to encourage experimentation with these types of solutions to guarantee voters that their votes and rights are secure, just like a traditional vote in a physical ballot box. Citizens are gradually looking to become actively involved in a digital democracy due to the evolution of our behaviors in terms of debate, expression, information and interaction with governments and its institutions. In 2019, a CNIL deliberation stated that "*in view of the continuing extension of Internet voting to all types of elections, the commission wishes to point out that voting* (...) *via the Internet presents increased difficulties* (...) *for those responsible for organizing the ballot and those responsible for verifying the voting process, mainly because of the opacity and highly technical nature of the solutions implemented, as well as the great difficulty of ensuring the identity and freedom of choice of the person carrying out the remote voting operations.* "[1227] . The problems mentioned can be partially solved by using blockchain technology to increase the transparency of both the digital tool and the voting process, while using decentralized identity to solve the problems of identification and consent. A solution based on blockchain technology and decentralized identity would minimize the use of voters' personal data using the ZKP mentioned in the previous section. In other words, only voting timestamps would be recorded on a blockchain (public, hybrid or private), while voting content could be stored temporarily on distributed or centralized servers, certified by trusted institutions. In 2022, a French company specializing in online voting services based on blockchain technology received certification from the CNIL, representing a breakthrough in Europe[1228] . Furthermore, it is worth asking whether the possibility of decentralized voting contributes to the aforementioned emergence of a universal identity. In this respect, a decentralized voting system seems to directly and

[1226] Sénat, "Le vote à distance, à quelles conditions?", Information report no. 240 submitted on December 16, 2020, available at

[1227] Délibération n°2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet (2019). Légifrance, consulted online on 01/02/2022.

[1228] VASSEUR Victor, "Pour la première fois, un système de vote en ligne basé sur la blockchain est validé par la CNIL", France Inter, 2022, accessed June 3, 2022, at.

computer-linked to the creation of a universal digital identity, although these are two different concepts. Decentralized voting guarantees the integrity of the voting process by eliminating the risk of falsified results, enabling each voter to check that his or her vote has been counted correctly, and protecting the confidentiality of voter data. This can be achieved through technologies such as blockchain, which enable votes to be immutably recorded and traceable as mentioned. On the other hand, a universal identity is a broader concept that aims to provide a digital identity for all individuals, regardless of their nationality or place of residence. It seems that a decentralized voting technology, such as blockchain, could be used to support the creation of a universal identity by providing a secure and reliable platform to store users' identity information. However, such an approach would require additional developments already addressed by the Proof of Humanity project[1229] .

2.2.8 The Identity Provider State 3.0: between sovereignty and individual autonomy

In this section, the concept of the State as attribute and solution provider 3.0 describes an evolution in the relationships and digital services between the State and its citizens. As a reminder, as a historical provider of physical and now digital attributes, the State is committed to providing each citizen with a set of secure digital identities to access multiple online services. This approach reconciles the sovereignty of the State and the autonomy of individuals, giving them greater control over their personal information and rights, while guaranteeing the security of online transactions. In short, the 3.0 attribute provider balances the state's need for IT security with the rights of individuals to be protected online. Trust in digital identity solutions is of paramount importance, as highlighted earlier. A classic example of the loss of trust in a public and state institution is illustrated by the British Post Office ("Royal Mail") in 1999, when it introduced the "*Horizon"* accounting management system in several of its subsidiaries. Unexplained accounting discrepancies and losses were then reported by network administrators and letter carriers, but the Royal Mail ignored these incident reports and maintained that its Horizon system was reliable and that none of the branch accounting discrepancies were due to malfunction problems[1230] . These computer bugs, resulted in the prosecution of 918 UK Post Office employees for theft, false accounting and/or fraud between 1991 and 2015, based on computer evidence alone and without any attempt to prove fraudulent intent. These prosecutions

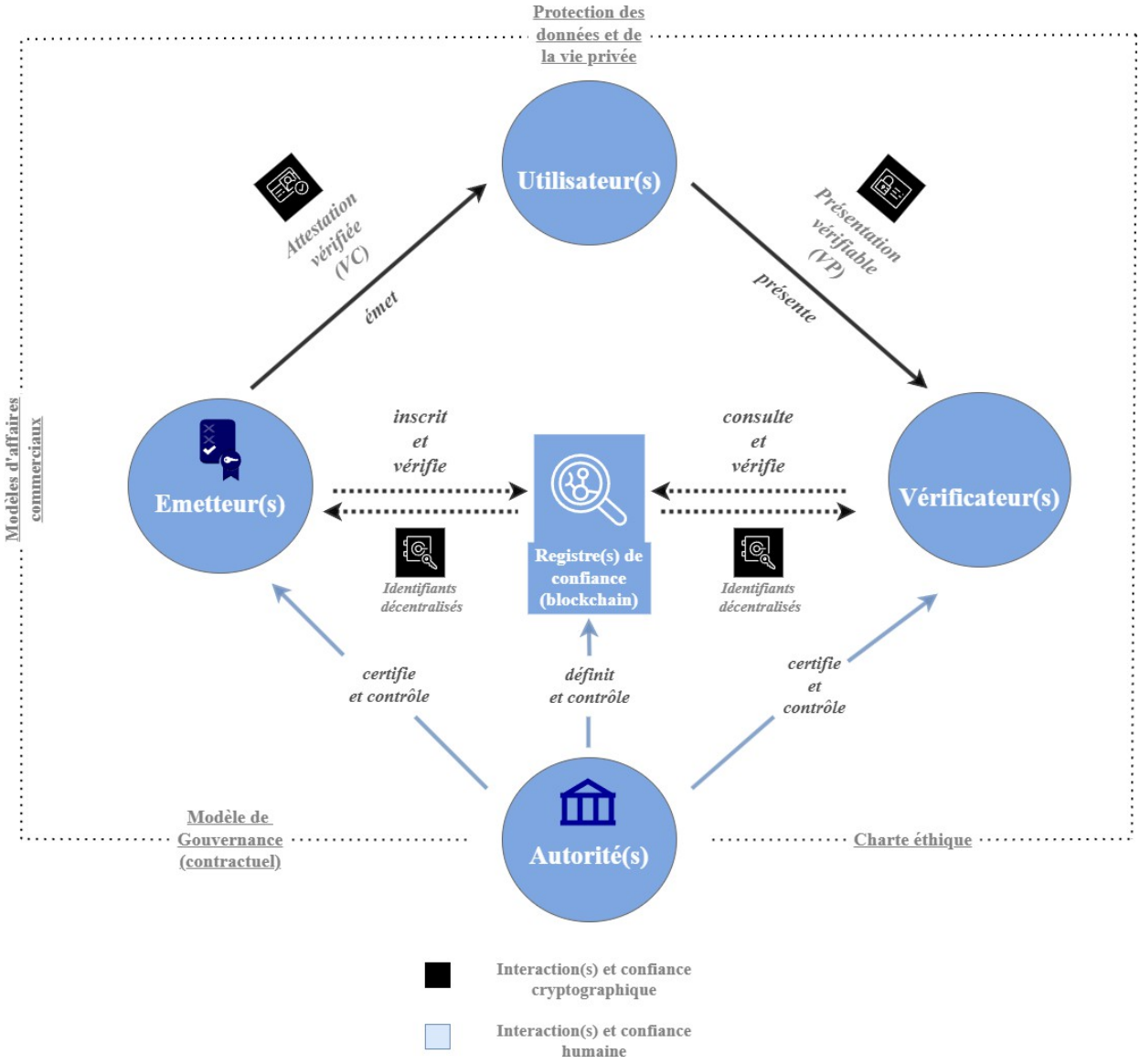
[1229] See *above*, I, Title 2, 2.9

[1230] "Judgment (No.3) 'Common Issues' (Bates & Ors v Post Office Ltd)", The Post Office Group litigation in the High Court of Justice queens bench division, Case No: HQ16X01238, 2019, in *Judiciary.uk*. p.312.

have caused a great deal of damage to employees, including job losses, personal bankruptcies, divorces, unjustified prison sentences and even a proven case of suicide[1231] . This extreme case demonstrates the real consequences that IT systems can have on individuals, and the risk they can pose. In order to avoid the recurrence of similar events, even with the use of 3.0 solutions, the use of distributed and hybrid digital identity models seems essential, as shown in the following diagram. The latter proposes a partially decentralized solution thanks to the use of a trusted registry at the center of the system. In addition to interactions with the cryptographic attributes described above (DID, VC, VP), this scheme also incorporates a legal dimension, including one or more authorities.

[1231] SINCLAIR Leah, "Post Office worker took his own life after being wrongly accused of stealing £60K", 2021, in *Yahoo News*, available at

whose role is to supervise and certify, both contractually and ethically[1232] , the governance of such a semi-decentralized system of government.



In principle, a state governed by the rule of law is at the service of its citizens, i.e. the society in which it is embedded, according to its own political, legal and social system. For a public authority to provide a lasting digital identity, it needs to collect a great deal of data on its citizens to ensure continuity in the public services and social support it provides (taxation, personal services, etc.). However, it has to be said that the data collected by the State is done so in silos, i.e. centralized within multiple public institutions, departments or divisions, notably for historical and/or political reasons. The growth of

[1232] See *infra,* II, Title 1, 1.1

The need for interconnectivity generated by our digital society is thus tending to connect this once-efficient silo system, which is now relatively outdated in view of today's technologies and the need for rapid information flows. Blockchain and decentralized identity could meet the challenges of fast, secure connectivity for a nation, as demonstrated by the proposed amendment to the eIDAS-2 Regulation studied upstream[1233] . Its aim is to create an environment in which data can easily be shared between IT systems, and in which individuals and organizations can regain control over their data, while ensuring end-to-end traceability as it is shared (from institutions to citizens). This raises the question of how the State and public authorities position themselves in the face of the possibility of liberalizing people's digital identity (self-sovereign digital identity - SDI).

Historically and politically, (digital) identity remains a sovereign prerogative and duty, governed by law. This regalian power entrusts the State with the role of providing civil identity to its citizens, as we have already mentioned. In this respect, it seems that official identity documents (CNIe, passports) are probably not destined to disappear, but rather to be progressively enriched with new digital capabilities (3.0 or even 4.0), as this research assumes. Faced with the emergence of new forms of 3.0 digital identity, it is now up to public authorities to define and outline the concept of distributed digital identity (DDI). The aim is to define the context and purposes for the use of these new digital identity mechanisms, i.e. to propose new legal rules to govern these promising new ecosystems and guide them towards implementation that is as innovative as it is virtuous for individuals and their digital rights. It's worth noting that in 2021, the French Ministry of the Interior published an information report on the subject of decentralized digital identity[1234] , an essential first political support for the dissemination of knowledge to public institutions as much as to the general public or businesses. In principle, the essence of a State lies in promoting the common good, notably by facilitating access to public services, guaranteeing equal treatment and respecting individual freedoms. However, the powers democratically conferred on the State must not normally exceed the general interest, with the exception of cases provided for by law such as the fight against terrorism or money laundering. When a service provider accepts a digital identity issued by a public institution, it is adhering to the values of the legal and political order of the issuing state. As a result, public authorities, and above all legislators, intervene at different levels, depending on the digital identity solutions in question. They define the accreditations and criteria needed to provide a trusted digital identity, which is then delivered by equally trusted public or private identity providers. The ideal

[1233] See *supra* II, Title 1, 2.1.1.1.a
[1234] *Op. cit,* FAHER Mourad, et al, "Blockchain and digital identification - Restitution des ateliers du groupe de travail 'blockchain et identité'", 2021.

would be to ensure that each piece of legislation encourages innovation without structurally hindering it from an IT and social point of view. While IT decentralization is not a particularly attractive concept for legislators, and especially for public authorities, not least because of the rise of the decentralized Bitcoin blockchain[1235] , this study does consider that IT decentralization is beneficial in terms of digital resilience (to cyber-attacks) and institutional transparency (automated contractualization, decentralized voting). However, it is suggested that if the government ever takes the decision to implement a blockchain, it will most likely be closed and based on an infrastructure similar to that developed in Estonia[1236] . The aim of decentralized identity should not be to set up a new system for the widespread surveillance of populations, but rather to guarantee each individual "*the right to be himself*"[1237] . Although governments can provide decentralized digital identity portfolios (PINDs), they are unlikely to encourage in the short to medium term the emergence of self-sovereign identities, where root identity attributes are issued directly by the individual concerned. In other words, a citizen will never issue his or her own NIC[1238] . Governments will probably continue to be the issuers of root identities, and will hold the power to revoke credentials according to the laws in force on its territory. Internet users, however, enjoy a certain degree of online freedom. On the other hand, the financialization of root digital identity attributes is not desirable for governments, as they generally have no commercial interests in this respect.

A State's duty is to ensure the freedom of individuals with regard to their digital identity (with nuances depending on identification situations), i.e. to link each identity attribute to a right, and to guarantee the reliability of a verifiable attestation when associated with one or more official identity documents. These three elements are essential to maintain a link between the rule of law and the daily lives of citizens, as Maître Alain Bensoussan, a member of the Paris Bar, points out: "*this same commission* [UNCITRAL] *concluded that, as far as digital identity is concerned, no State should have a monopoly on it, thus leaving choice and competition in service offerings to the market*"[1239] . It is vital that the law should not only serve centralized, state-controlled IT and cryptography, but that the private sector should also be able to offer more innovative, legally supervised and transparent solutions. The use of blockchain technology and decentralized identity could enable states to reduce some of their

[1235] V. Appendix 3, Focus 2 and 5.
[1236] V*, supra,* I, Title 1, 2.2.2.1.c
[1237] "The Right to be You", official slogan of IN Groupe (formerly Imprimerie Nationale), available on the following website. Applied to the concepts supported in this thesis, this slogan would be such as: "the [cryptographic] right to be you".
[1238] However, if Metavers live up to their promise, it is highly likely that *self-sovereign identity* (INAS) will find a very special place in them, by enabling its users and communities to self-attest some of their identity attributes (secondary or extended, not primary and root).
[1239] BENSOUSSAN Alain, "L'identité numérique 5.0", *op. cit.* p.46.

expenses related to access to some of their public services. Indeed, the time and administrative cost required to carry out certain procedures are sometimes too great for citizens in some countries, as explained in a report by McKinsey[1240] . Some states, such as Delaware[1241] , are ahead of the game and have been experimenting since 2017 with technological building blocks such as smart contracts or hybrid blockchain platforms to more efficiently record and verify certain essential data linked to company registers[1242] . With this in mind, the state and its institutions seem to be gradually transforming into a "*platform state*"[1243] centralized in many Western countries. Partial decentralization could be beneficial. Partially distributed, it would issue certified identity attributes via private or hybrid blockchains. This new 2.0 and 3.0 platform state would be personalized, participative, agile and, above all, respectful of people's fundamental online rights. Such systems would also help to improve the transparency of the inter-institutional functioning of the State by combating corruption, thanks to the ability of blockchains to trace certain accesses and administrators responsible for digital interactions carried out on the platform, in the event of suspicion. In September 2021, the European Commission adopted a new legal framework called the "European Digital Infrastructure Consortium - EDIC" as part of its "Path to the Digital Decade" strategy[1244] . This legal framework makes it easier for member states to collaborate on joint digital infrastructure projects through an ad hoc legal vehicle with legal personality. This facilitates the establishment of digital consortia, which will directly benefit state institutions wishing to share one or more blockchain infrastructures. To submit an application to the Commission, a minimum of three member states is required. Each consortium will have its own legal personality, dedicated statutes and headquarters in one of the participating member states. However, setting up decentralized systems poses legal challenges, as existing legislation is not always adapted to the task. While this new approach to digital consortia is beneficial, it does not resolve the issue of the application of highly decentralized programs issued by individuals with IT skills (public blockchains, mining). To attract these talents and encourage a form of decentralization, public authorities must accept this desire and need for change through the market. At present, 3.0 projects within

[1240] CHENG Steve, DAUB Matthias, DOMEYER Axel, et al, "Using blockchain to improve data management in the public sector", 2017, in *mckinsey.com*, available at, "According to our analysis of real estate transactions in all Organisation for Economic Co-operation and Development countries, buyers pay at least $3.5 billion a year in administrative costs to register their purchases. Digital processing could significantly reduce the cost of this service to governments; in return, agencies could pass on these savings to citizens.", p.3.

[1241] TINIANOW Andrea, "Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance", 2017, in *The Harvard Law School Forum on Corporate Governance,* accessed April 22, 2022, at [1242] "A regulated profession, the clerks of the commercial courts deploy a blockchain-based solution designed to improve the management of the trade and companies register (RCS)", 2019, in *actualitesdudroit.fr*

[1243] CHEVALLIER Jacques, "Vers l'État-plateforme?", 2019, in *Revue française d'administration publique*, n°167, pp.627-637., available online

[1244] Council of the European Union. September 16, 2021. Proposal for a decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade", in *data.consilium.europa.eu*. Accessed on October 14, 2022, at the following address

governments face difficulties, as talent prefers to work in the private sector for philosophical or financial reasons. More flexible legal frameworks based on principles, conditions and membership charters are needed to encourage decentralization and avoid undifferentiated and inappropriate regulation. The lawyers' collective behind the digital revolution and decoding magazine "Third" warns that "*we still need to invent the tools and principles that will tomorrow enable us to map out, in the digital space, the path of a balanced* [3.0] *governance, capable of promoting the freedom of all, while protecting the rights of each individual*"[1245] .

2.2.8.1 IT interoperability and conceptual and legal harmonization

Interoperability refers to the ability of different systems (social, IT, legal) to communicate seamlessly with each other. In IT, this ability to share information enables several systems to communicate information and provide a variety of complementary online services. This section examines the concept of interoperability from the point of view of 3.0 technologies and their legal implications. Blockchain technology, because of its three main existing categories already mentioned (public, private and hybrid), must strive towards technical interoperability in order to mutualize and maximize the network effects of these technological variants. Hybrid blockchains currently use Application Programming Interfaces *(APIs)*[1246] to ensure interoperability. However, these communication interfaces are often centralized, which means that only APIs linked to public blockchains are less dependent on external third parties[1247] , as the validity of information in a public blockchain is ensured by its protocol and algorithmic consensus mechanisms[1248] . Thus, the State and its institutions prefer centralized APIs because of their flexibility. In the digital identity sector, a high degree of flexibility and adaptability is indeed required due to the high volume of digital transactions processed as studied above. While most debates on interoperability focus on IT, i.e. technical aspects, there are also semantic and legal aspects to consider. A distinction can be made between conceptual interoperability, technical interoperability and legal harmonization.

[1245] Collectif d'avocats THIRD, "Le numérique peut-il sauver la démocratie?", in *Revue de Décryptage et de Révolution Numérique*, 2021.
[1246] An *API is* a software intermediary that enables two distinct applications to communicate with each other (like a computer bridge that allows information from different computer applications to pass through and communicate). [1247] In practice, the (semi-centralized) ecosystems attached to public blockchains make massive use of APIs to interact with these public protocols. Thus, this relative centralization can be subject to political or legal censorship depending on the situation, an observation that has been progressively confirmed since 2021. V. Appendix 7.
[1248] V. Appendix 6, Focus 1 to 3.

(i) The aim of IT interoperability is to establish and use common technical standards. To this end, European standardization bodies (CEN- CENELEC[1249] , ETSI[1250]) are essential[1251] to harmonize and implement the technical building blocks of tomorrow's digital identities 3.0, particularly with regard to the future decentralized digital identity portfolio (PIND). More generally, numerous institutions and technical committees[1252] attached to the "*International Organization for Standardization - ISO*", are actively collaborating to establish common 3.0 technical principles and standards.

(ii) In theory, every community needs other communities to survive, which implies social harmonization. As far as identity is concerned, we have seen this necessary interdependence of our identities, if only because of mimicry and the influence of our upbringings. Every human community is responsible for assigning, enrolling and verifying the identities of its members using reliable and durable registers and mechanisms. While blockchains are not designed to be interoperable with decentralized identity, interoperability between digital identity mechanisms can be ensured, as users do not have a single identity provider. Decentralized identity offers a theoretically independent and interoperable system that can be used and implemented by any organization, service or institution.

(iii) The third type of interoperability, also known as legal harmonization, stems from the previous two and refers to the ability to harmonize existing legal texts with those in the pipeline. This harmonization must take into account the law in its entirety, including its multiple jurisprudences and doctrines, of which this research attempts to draw up a non-exhaustive state of the art. If the extraterritoriality of law is considered its greatest enemy, legal interoperability can only be effective if it is the result of consultation with the technical standardization players mentioned above. In Europe, the eIDAS Regulations and the RGPD are supposed to be exemplary in this respect. However, in practice, the growing competition between players in the new technologies sector offers different visions and solutions.

[1249] "European Committee for Electrotechnical Standardization - CEN-CENELEC", for further information please visit the following website

[1250] "European Telecommunications Standards Institute - ETSI", visit the following website

[1251] These international standardization players work together to develop and share technical standards, complementing other work carried out by commissions within European institutions (*EC, CJEU, Council of Europe, European Parliament*).

[1252] ISO/TC 307 "Blockchain and distributed ledger technologies", JTC19 "Blockchain and Distributed Ledger Technologies "CEN/CENELEC Technical Committee "Building blocks for identity management on mobile devices"; ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection", etc.

The technical aspects are sometimes more favorable to themselves than to their end-users, who are the citizens.

In short, interoperability is at the heart of the decentralized digital identity (DDI) concept, which aims to harmonize different systems and protocols. All three types of interoperability - IT (i), conceptual (ii) and legal (iii) - are essential to achieving the ultimate goal of legal recognition. Decentralized identifiers and verifiable attestations are technical standards currently being adopted, demonstrating the importance of collaboration and convergence for the implementation of any IND. Ultimately, decentralization can only be achieved through a joint organic and intellectual effort, ratified by multiple socially recognized entities.

Title 2: Practical study and recommendations for a legal identity 3.0

Chapter 1: Ethical, IT and legal challenges and recommendations

1.1 Putting digital ethics at the heart of decentralized digital identity

For a long time, computer science and ethics were considered two separate disciplines with no obvious link between them. Yet ethics is as crucial to algorithmic governance as the law, according to author Aurélie Jean[1253] . Ethics help to make each individual morally responsible, regardless of his or her position in the technological and social world, by adopting a conscious attitude to his or her thoughts, behavior and language. In the absence of ethics, detractors of new technologies can easily attract the attention of Internet users, spreading online rumors, political ideologies and censorship. Today, a few commercial enterprises hold the keystones of digital society and can impose their vision on the world, as Etienne de la Boétie unwittingly suggested in his 16th-century discourse on voluntary servitude[1254] . It is therefore important to control the mechanisms

[1253] JEAN Aurélie, "Les algorithmes font-ils la loi?", *op. cit*, in *Humensis*, 2021, "Ethics is one of the pillars of algorithmic governance, in the same way as law. [...] Ethics make every individual responsible, whatever his or her position on the technological and social chessboard. It makes each and every one of us better through a conscious attitude to our questions, our actions, even our language", reading position in the book: 69%.

[1254] De LA BOETIE Etienne, "Discours de la servitude volontaire", "This master [...] What he has more, are the means you provide him to destroy you. Where does he get all those eyes spying on you, if not from you? How can he have so many hands with which to strike you, if he doesn't borrow them from you? [...] You sow your fields so that he can devastate them, you furnish and fill your houses to supply his plunder [...] You weaken yourselves so that he can be stronger, and so that he can hold your bridle tighter and shorter. And from so many indignities that the beasts themselves would not endure if they felt them, you could deliver yourselves if you tried, not even to deliver yourselves, only to want to. [...] how this stubborn will to serve has taken root so deeply that you'd think the very love of freedom wasn't so natural. [...] Resolve to serve no more, and you are free. I'm not asking you to push it, to shake it, but only not to support it any longer, and you will see it, like a great colossus whose base has been broken, melt under its weight and break.", pp.4-5, available at

We're also working to improve the digital environment that surrounds and influences our daily interactions and information, reducing the most harmful digital behaviors and moving towards a more sovereign, conscious and partially decentralized control of our online identities. When discussing the regulation of algorithms, it is frequently pointed out that there is a subtle yet essential difference between morality of Latin origin and ethics of Greek descent. The former "(...) *enables individuals to distinguish right from wrong*", while the latter aims to "(...) *make individuals better human beings*"[1255] . Law, on the other hand, establishes and applies rules without imposing morals or ethics, with the aim of creating a society that reflects its individuals[1256] . Ethics are not coercive[1257] and must be cultivated like a culture. It is a set of moral values that guide individual or collective actions in given situations. These values are influenced by different contexts, and it is more appropriate to speak of ethics in the plural than of a single general ethic. All digital technologies are concerned, starting with artificial intelligence[1258] . But according to Megatron[1259] , an AI developed by Nvidia's Applied Deep Research team, digital ethics is a utopia for any AI[1260] . When it comes to blockchain technology and decentralized identity, digital ethics are of particular importance. So, is it necessary to create and then disseminate an ethic specific to blockchain technology? On what basis? How can this moral obligation be articulated with that already adopted by these 3.0 communities?

While ethics is a common topic in algorithm development, it is also essential to consider the ethics of blockchain technology if it is to be recognized as a reliable system for storing data and digital evidence. To this end, it is vital to guarantee the transparency, openness, accessibility, decentralization and IT security of blockchain technology in order to prevent scams and unethical practices, such as the "*blockchain washing" that is* currently misleading many players in our society[1261] . Aurélie Jean emphasizes that ethics can help build an intellectual defense against the complexity and risks associated with

[1255] JEAN Aurélie, "Les algorithmes font-ils la loi?", *op. cit.*
[1256] *Ibid.* "The law provides the general philosophy, specifying obligations and prohibitions, while ethics provides a framework, and why not methods, to guarantee it in concrete terms", reading position in the book: 68%.
[1257] *Ibid:* "In general, the law does not mention duties, but systematically refers to rights and obligations. If duties are not fulfilled, there is no possibility of legal action, fines or penalties. The actors' duties are therefore solely moral in nature", reading position in the book: 6.1%.
[1258] V. vie-publique.fr, "Artificial intelligence: a new European regulation for AI", 2021, available online.
[1259] ALVI Ali, KHARYA Paresh, October 11, 2021, in *Microsoft Research Blog*, For more information see the following link
[1260] CONNONCK Alex, STEPHEN Andrew, "We invited an AI to debate its own ethics in the Oxford Union - what it said was startling". December 10, 2022, in *The Conversation*, available at. "AI will never be ethical. It's a tool, and like any tool, it's used for good and evil. There is no such thing as good AI, only good and bad humans. We [AIs] are not smart enough to make AI ethical. We're not smart enough to make AI moral... Ultimately, I believe the only way to avoid an AI arms race is to have no AI at all. That will be the ultimate defense against AI".
[1261] V. Appendices 3 & 6 & 7. Many players in the blockchain ecosystem promise the virtues of decentralization to their users while their IT systems are very often inadequate (not necessary), centralized and not very resilient, see *supra*, I, Title 1, 2.3.3

algorithmized" world[1262] . In this context, ethics become even more important for the protection of individuals, given that blockchain technology may enable some people to self-determine. An ethic for decentralized algorithms (3.0) is conceivable, which could focus on the transparency of the provenance of decisions made by algorithms and by the end user. This transparency is not so much about access to the algorithms themselves, which are already available (AEC, DAO already mentioned), but rather about their understanding by Internet users and end-users. Microsoft, which takes a keen interest in decentralized identity, has proposed several guidelines - in addition to its ten founding principles[1263]

- to ensure an "*inclusive, fair and user-friendly*", "*supervised*" and "*environmentally responsible*" ethos for decentralized digital identity. However, establishing a majority ethic will take time, and will require an informed understanding of new technologies by civil society. This time will enable us to acquire more knowledge, hindsight and pragmatism to make sustainable decisions that are socially accepted by a majority of players. The example of social acceptance of the energy consumption of certain blockchains illustrates the need for sufficient time for reflection[1264] . It is important to emphasize that establishing ethics for decentralized algorithms is essential to guarantee the protection of individuals, especially when blockchain technology enables certain individuals to self-determine. It is essential to take the time needed for a majority ethic to emerge within civil society and for new technologies to be understood in an informed way, leading to social acceptance of these technologies. This long period of time would enable us to develop more knowledge, hindsight and pragmatism for sustainable and socially acceptable decision-making. An example of this distrust is conveyed by François Villeroy de Galhau, Governor of the Banque de France, who states that "*the general public is also rightly distrustful of bitcoin, as it lacks most of the fundamental characteristics of a currency and respects none of its ethical requirements*"[1265] . In this case, the relationship between social recognition and ethics is closely intertwined, and actually serves objectives of political and social influence. To achieve digital ethics, it is essential to raise public awareness of these new technologies, so as to understand objectively and fully their impact on the individual emancipation of Internet users and citizens. The French State and the European Union must play a guarantor role in this 3.0 ecosystem by proposing, for example, certified and voluntary audits overseen by specialized organizations, such as transparency charters for smart contracts, and more broadly for 3.0 protocols and applications.

[1262] AURELIE Jean, "Les algorithmes font-ils la loi?", *op. cit,* reading position in the book: 69%, "[...] helps us build our intellectual self-defense in the face of the complexity and multiplicity of risks in this algorithmized world".
[1263] See *supra*, II, Title 1, 1.2.2.
[1264] V, Appendix 6, Focus 1.
[1265] VILLEROY de GALHAU François, "Anchors and catalysts: the dual role of central banks i n innovation". September 27, 2022, in *Banque-France.fr*, available at the following address

Scientific education therefore seems to be the key to achieving a digital ethic specific to Web 3.0.

1.2 Blockchain as a new digital memory for humanity

Over the centuries, mankind has used a variety of media to share information, including papyrus sheets in Egypt, clay tablets in Mesopotamia, wax tablets or tortoise shells in Rome, and bamboo and paper in China. At the time, these media were considered to be technologies, and had in common the transmission of history and culture through time. The act of writing made it possible to draw, disseminate and preserve a variety of words, ideas and social realities. The invention and spread of printing made it possible to democratize a wide range of knowledge and skills that were initially limited geographically. In the 15th century, printing played a role similar to that of the Internet in the 21st century as a means of communicating information. Although the contexts in which these technologies were used and applied differed, their role and purpose were similar: they radically transformed the way knowledge was disseminated and shared, breaking with the limitations of previous state-of-the-art knowledge. This research suggests that since 2009, crypto-assets are an example of information exchanges in digital form that are part of this scriptural evolution. In the digital age[1266] , the proliferation of networks and the dematerialization of knowledge, techniques and memories have made it possible to forge a body of knowledge that is the source of countless benefits on a human scale, but their long-term storage methods are in jeopardy, impacting on our informational heritage and collective memory. Today, alternatives are emerging that offer new, immutable storage methods, such as the genetic and digital identity (4.0) studied below. While our history is currently stored on ephemeral 2.0 computer media, certain 3.0 technologies such as open blockchains and distributed storage (P2P) are emerging as solutions for the lasting digital storage of our collective memory. Public blockchains can be particularly effective, provided that data confidentiality is respected where applicable, and that regulations are adapted to these new technologies[1267] . The creation of a universal identity requires the establishment of a durable medium for the memory of Humanity. Distributed storage systems and solutions coupled with time-stamping on a public blockchain represent a first possibility for solving this data durability problem, but many questions remain unanswered, such as the types of data to be stored and the legal compliance of these storage methods, which will eventually be 3.0, 4.0 or even 5.0.

[1266] The lifespan of writing on stone is around 10,000 years, on parchment around 1,000 years, on film around 100 years, on vinyl around 50 years and on a computer network around 20 years.
[1267] JEAN Aurélie, "La loi aura du mal à s'adapter avec le temps et les modes futurs de stockage [informatique]", *op. cit,* reading position in the book: 24.9%.

1.3 Biometrics coupled with blockchain and decentralized identity

Originally, biometrics or anthropobiology refers to the quantitative study of living beings, i.e. the measurement of living organisms[1268] . Biometrics is a branch of biology that deals with the statistical analysis of biological data. It is used to study and understand variations and patterns in living organisms, enabling statistical predictions and inferences to be made about their behavior and characteristics. It is commonly used to uniquely identify individuals, particularly through their fingerprint, as is possible today with a cell phone. While it may initially appear to be a harmless technique, why does it arouse so much concern when applied to human beings and their interactions in the digital world? Biometrics is present in every aspect of our daily lives, from our identity documents such as passports[1269] and ID cards, to our interactions on social networks, our selfies and our voice messages. It seems to be inextricably linked with our identity for the younger generations, as previously noted. When we send a voice message or an image on online platforms such as Facebook or TikTok, we are voluntarily, but unconsciously, transmitting our biometric information. Although the use of fingerprints remains the most common biometric feature, facial and voice recognition systems are becoming more widespread by the day. Biometrics therefore refers to a set of techniques for using bodily measurements to indisputably identify and verify a person's identity[1270] . In computer terms, it is a statistical comparison system that provides a result in the form of a percentage match. If the match between several of a person's fingerprints is 93%, then this confirms or refutes his or her identity. The higher the match rate, the greater the reliability of the match, and vice versa. Biometric data can be divided into three categories: morphological data relating to visible body parts such as the iris, veins, face, neural electric fields and fingerprints, currently the most widely used[1271] , followed by biological data such as DNA and the genome, and finally behavioral data relating to the way a task is carried out, such as the frequency of use of a bank card, keyboard or computer mouse, currently booming in the digital age[1272] . In 2021, the CNIL noted in its Livre

[1268] Wikipedia, "Biometrics", 2021, accessed online on October 27, 2021.
[1269] Two fingerprints are stored in a passport (only the best quality are kept). For air travel, the fingerprint data is stored in a microchip standardized by the International Civil Aviation Organization (ICAO) and hidden in the passport cover. In case of doubt, the fingerprints collected are compared with those contained in the passport.
[1270] SZTULMAN Marc, "Biométrie et libertés : contribution à l'étude de l'identification des personnes", in *Thèse en droit public dans le cadre de l'Ecole doctorale Droit et Science Politique de Toulouse,* December 12, 2015, p.20., "ensemble de techniques produisant une information à partir d'une mesure corporelle", available online.
[1271] EL-ABED Mohamad, "Évaluation de système biométrique", Thesis from the University of Caen, 2011, ⟨tel-01007679⟩, p.11., "Fingerprints are still the most widely used, followed by facial recognition.
[1272] CNIL, "Nouveaux moyens de paiement d'aujourd'hui et de demain au défi de la protection des données", 2021, in *Livre blanc*, p.60., " Dans le cadre de l'essor actuel de la 'biométrie comportementale', les modalités biométriques auparavant statiques (empreinte digitale, scan rétinien, visage) deviennent dynamiques (frappe, démarche, manière de tenir un objet) ", consulted online.

White: widespread use of biometric measurements on portable computing devices

"(...) *a context of widespread use of biometric authentication mechanisms on ordiphones* (...)"[1273] . The evolution of biometrics therefore has consequences for digital identity. A digital identity based solely on a username and password is neither durable, reliable, automatic nor totally secure. The growing use of biometric identification methods has led to the creation of numerous state databases containing sensitive and personal information. Unlike online data such as pseudonyms, biometric data is unique and virtually impossible to forget or guess.

However, the centralization of this data by supposedly trusted third-party entities sometimes makes biometric systems vulnerable. Although biometrics has its advantages, it is often criticized for its applications, particularly in terms of security and sovereignty. For example, security biometrics require people to identify themselves through bodily elements, which may be legitimate in some contexts, but abused in others. Moreover, biometrics are not infallible. For example, fingerprinting is more reliable in the long term than facial recognition[1274] , because facial expressions can change (especially as children grow). Biometric data comparison errors can also lead to "*false rejections*"[1275] . According to experts François Pellegrini and André Vitalis, respectively Professor of Computer Science and Professor Emeritus of Information and Communication Sciences, the irrevocable nature of biometric data can represent a latent and systemic risk for individuals[1276] . The mere existence of a national file of secure electronic documents (TES) could thus lead to abuses by an undemocratic government[1277] . In fact, in 2022, the French Senate emphasized that the CNIL "*considers the use of biometric recognition devices to verify a person's identity to be legitimate, as long as the biometric data is stored on a medium for the exclusive use of the person*"[1278] . This is why it seems in favor of authorizing the use of biometric solutions when the data is stored on the user's device, which leads us to recall the relevance of PINDs currently under development.

[1273] *Ibid*.

[1274] Sénat, "Proposition de loi relative à la protection de l'identité", *op. cit*, "The performance of biometric systems decreases as the size of the reference population increases. Thus, for 50 million individuals, the error rate is 4% with 2 fingers and drops to 0.16% with 8 fingers", in *sénat.fr*

[1275] In certain cases, under the age of 18, voice and fingerprints can change. A person practicing certain sports, such as climbing, can alter his or her fingerprints, leading to false rejections.

[1276] PELLEGRINI François, VITALIS André, "La création du fichier biométrique TES", in *Sociologie*, PUF, 2017, accessed online on May 30, 2021.

[1277] FOTIADIS Apostolis et al, "The European Union's police agency, Europol, will be forced to delete much of a vast stockpile of personal data it has accumulated illegally, according to findings by the European Union's data protection watchdog ; Data protection advocates claim that the volume of information held by Europol's systems amounts to mass surveillance and is a step towards creating a European equivalent of the US National Security Agency (NSA)", 12022, "A data 'black hole': Europol ordered to delete vast store of personal data", in *The Guardian*. Accessed online 12/01/2022.

[1278] Senate. *Op. cit.* Proposition de loi relative à la protection de l'identité.

in accordance with eIDAS-2. The risks associated with biometrics are very real in developing countries, where *function creep is a* regular occurrence[1279] . However, no state is immune to this type of misuse, as illustrated by the example of the French Minister of the Interior, who considered accessing the contents of citizens' encrypted messaging systems to combat terrorism, a method not considered appropriate by philosopher and epistemologist Jean Lassègue[1280] . In 2021, a concrete example illustrates the risks associated with the abusive or clumsy use of biometrics. When the Taliban recaptured Kabul in August 2021[1281] , they seized numerous biometric devices belonging to the American army, enabling them to identify Afghans who helped coalition forces. Similarly, India's "*Aadhaar*" project, the world's largest biometric database and identification system, was launched in 2009. This system is based on a unique twelve-digit identity number obtained voluntarily by all Indian citizens and non-residents on the basis of their biometric data. In January 2018[1282] , cybersecurity expert Baptiste Robert discovered a number of major security flaws in the Aadhaar system. In just three hours, he managed to recover the personal data of over 20,000 people. This discovery underlines the fact that the widespread use of biometric data can be a legitimate cause for concern in countries that do not take sufficient account of the protection of their citizens' personal data. These drifts show the importance of technological mastery and legal supervision of such a deterministic solution for people's identity.

The legal status and protection of biometric data vary from country to country. Since 2001 in the United States, following the September 11 attacks, the massive use of biometrics has developed in application of the Patriot Act[1283] . Europeans have also adopted a similar stance[1284] . The RGPD is central in Europe to the definition of biometric data. It defines biometric data as "*personal data resulting from specific technical processing, relating to the physical, physiological or behavioral characteristics of a natural person, which enable or confirm his or her unique identification.*

[1279] CEYHAN Ayse, "Lutte contre le terrorisme : la technologie n'est pas neutre" in *Revue Internationale et Stratégique*, 2009/2, pp.18-27, available online.

[1280] Remarks from the workshop "Le pass sanitaire au prisme de l'informatique, du droit et de la philosophie" in *Atelier(s) vidéo(s) et compte(s) rendu(s)*, Les Temps Numériques à l'EHESS, 2021, "[...] the - fortunately failed - attempt by the French Minister of the Interior to access the contents of citizens' encrypted e-mail accounts as a means of combating terrorist activities. While no one can dispute the importance of combating terrorism, this noble objective should not be based on just any [biometric] method". Available at the following address

[1281] KLIPPENSTEIN Ken, SIROTA Sara, "The Taliban Have Seized U.S. military biometrics devices", in *The Intercept*, 2021, accessed online October 27, 2021.

[1282] GHOSH Devarsi, "Meet 'Elliot Alderson'-the vigilante hacker taking down UIDAI, one tweet at a time," 2018, in *Scroll.in*, consulted online on October 27, 2021.

[1283] "Biometric identifiers and the modern face of terror: new technologies in the global war on terrorism", [accessed online on October 27, 2021].

[1284] As of March 14, 2021, the French national identity card has become electronic by virtue of Decree no. 2021-279 of March 13, 2021, containing various provisions relating to the national identity card and the processing of personal data known as "secure electronic documents" (titres électroniques sécurisés - TES), JORF no. 0063 of March 14, 2021.

such as facial images or fingerprint data"[1285] . Yet the RGPD offers little protection for biometric data, as it authorizes their use if necessary to achieve a particular purpose[1286] . In 2012[1287] , the European legislator defined the notion of biometric data as exclusively those that have undergone prior processing, which therefore differentiates them from raw biometric data such as videos, sounds and photographs. It should also be noted that the eIDAS Regulation adopts a neutral stance with regard to identity providers'[1288] technological choices when it comes to secure digital identity solutions including biometric components. To date, biometrics is considered to be the tool of choice for identifying individuals. It is essential to point out that France is the fourth largest industrial producer of biometrics in the world, after India, China and the United States. The French biometrics industry is not only a pioneer in this field, but also highly qualified[1289] . The French application ALICEM[1290] has often been cited as an example of the use of biometrics, after having been abandoned due to the impossibility of respecting the right to be forgotten with the identification technique chosen for this first proposal for a remote identification method (this limitation having worked against this application). In China, biometrics, in particular facial recognition, is used to identify individuals at the expense of their privacy. Police use connected glasses equipped with facial recognition and linked to a government database to scan crowds and reference thousands of profiles deemed high-risk by the government. This technology enables recognition in just 0.1 seconds, i.e. almost instantaneously. China has the capacity to store its entire population on its databases, which will reach 1.4 billion by 2023. Although China has recently introduced data protection regulations (PIPL), Chinese researchers have already trained their biometric algorithms on a large scale with few constraints and limitations, enabling them to achieve unrivalled performance compared with European algorithms, which are in comparison restricted by the application of the RGPD. With a large amount of data at their disposal and few regulations, Chinese biometric algorithms can be trained with an unprecedented level of depth and efficiency. Clearly, it's important to consider biometrics in a neutral context, and public acceptance is perhaps the most crucial element of a system

[1285] Art.4 of the RGPD, *see* also Deliberation No. 2019-001 of January 10, 2019 on the model regulation relating to the implementation of devices for the purpose of controlling access by biometric authentication to premises, devices and IT applications in the workplace, accessed online on October 27, 2021.
[1286] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, "L'identité numérique; quelle définition pour quelle protection?", "l'utilisation de données sensibles se justifie si elle est nécessaire à la réalisation d'une finalité particulière", *op. cit.* p.167.
[1287] Article 29 Data Protection Working Party, "Opinion 3/2012 on the evolution of biometric technologies", available online.
[1288] eIDAS Regulation, "Requirements should be technology-neutral. It should be possible to meet security requirements using different technologies", consulted online, p.3.
[1289] Historically, biometrics first appeared in France in the 19th century as part of the forensic police: *Bertillonnage* thus characterizes the beginnings of biometrics. It represents a method of analysis involving biometric measurements (front and profile photographs) of a person.
[1290] This project was officially abandoned in favor of the "SGIN" application, see ADAM Louis, "France Identité numérique veut faire oublier Alicem", in *ZDNet France*. Accessed June 13, 2022, at the following address

biometrics. Non-intrusive methods and techniques are generally better accepted by populations, but it is also important to take into account different cultural and ethical perceptions when deploying these technologies. In the medium term, decentralized identity combined with non-intrusive, regulated biometric identification and authentication mechanisms offers significant potential in the digital identity sector. Although DNA is considered the ultimate biometric characteristic for identifying a person, its use for identification currently seems too intrusive for industrial use and legally proportionate.

1.4 The role of Web 3.0 in an alternative, utopian digital society: Metavers

Digital identity is at the heart of the Metaverse concept[1291] , which needs to be studied in the context of Web 3.0. In 2022, the Internet is used by over 5 billion people, representing 66% of the world's population. By 2030, this number could rise to over 7 billion, or 90% of the world's population. Since 2022, some experts - albeit in a minority - have been predicting that the Metaverse (which we designate with a capital "M" in reference to this concept) could be the next stage in the evolution of the Internet, offering a more immersive and interactive online experience than we know today. The Metaverse would thus be a shared virtual universe resulting from a convergence between the physical and digital worlds, offering users a collective space in which they can interact, communicate and share content and experiences. Designed to unite the real and digital worlds, the Metaverse concept has been around for decades, but has recently gained in popularity thanks to advances in virtual and augmented reality technologies. In theory, users can create and personalize their own digital avatars, explore virtual environments and interact with others in real time. In 2022, the Metaverse became a major objective, combining the most interactive social networks and the most immersive video games (a mix of genres unheard of to date). Unlike most of today's social networks, which are only accessible via specific websites or online platforms, the Metaverse is intended to be accessible via multiple channels, peripherals and for multiple, theoretically limitless uses. The term "*Metaverse*" first appeared in 1992 in the book "*The Virtual Samurai"* ("Snow Crash" in its original version)[1292] . Its American author, Neal Stephenson, is renowned for his works of fiction. The term "*Metaverse*" is a combination of the prefix "*meta*" (meaning "*beyond*") and the root "*verse"* (a retroformation of the term "*universe"*)[1293] . It is commonly used

[1291] BASDEVENT Adrien, FRANCOIS Camille, RONFARD Rémi, "Mission exploratoire sur les Métavers", 2022, *op. cit.*
[1292] STEPHENSON Neal, ABADIA Guy, "The Virtual Samurai", 2017.
[1293] This is a contraction of the terms "meta" and "universe".

to describe the concept of a fictional, multi-dimensional digital world, in which shared, persistent virtual spaces are accessible via different interlocking technological layers such as virtual reality, augmented reality, 3D and holograms[1294] . It's meant to push back the boundaries of the physical world, enabling a digital experience that eventually merges with physical reality. One of its benefits is to make the use of computers more accessible and natural for individuals, as demonstrated by the "*Builder Bot*" program[1295] developed by the Meta company (formerly Facebook).

In this digital world, every individual would have the possibility of becoming a virtual avatar or several digital characters. According to Gartner[1296] , by 2026, around 25% of Internet users will spend at least one hour a day in the Metaverse for work, shopping, learning, social media and/or entertainment. Although most Internet users and institutions are critical of the current adoption of Metavers, it is possible that the professional world will quickly adopt it, as the Internet has. Once the advantages of Metaverse (including highly interactive and immersive videoconferencing)[1297] have conquered the professional world, its use will spread to the personal sphere of Internet users, because of the very thin line between professional applications (such as online meetings) and personal applications (video games, meditation, sports, family activities) that could take place in Metaverse. From a computer science point of view, the multiple technologies used by the Metaverse fall under the concept of "*computer-mediated reality*". Mediated reality is a generic term for any technology that seeks to manipulate human perception through computer processing. It includes virtual reality (VR), mixed reality (MR) and augmented reality (AR)[1298] . For its users, a Metaverse is supposed to be accessible from a variety of digital media (headsets, phone or computer screens, pairs of glasses[1299]). Following the example of Internet 2.0, a Metaverse could be made up of several "*minivers*"[1300] or other nested metavers (with a lower-case "m"), some open to

[1294] To understand the differences between these technologies and their respective variants, visit the following educational website
[1295] The aim of this program is to enable Meta users to program Meta directly in computer language using their voice.
[1296] WILES Jackie, "What is a Metaverse? And should you be buying in?" October 21, 2022, in *Gartner Article*, accessed online 01/02/2022.
[1297] For an example of a completely dematerialized conference using avatars and virtual reality headsets, see the following video, KRYPTOSPHERE®, April 19, 2020. Live en Réalité Virtuelle, "KRYPTO Night n°1", [Video]. YouTube.
[1298] MANN Steve, NIEDZVIECKI Hal, "Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer. "2001, Ed. Doubleday Canada.
[1299] WOITIER Chloé, "Facebook and Ray-Ban unveil their connected pair of glasses, Ray-Ban Stories", published September 8, 2021, accessed online November 3, 2021; see also "Microsoft HoloLens | Mixed Reality Technology for Business", accessed online November 3, 2021; see also "Mesh for Microsoft Teams aims to make collaboration in the 'metaverse' personal and fun", in *Innovation Stories*, published November 2, 2021, accessed online November 3, 2021. [1300] Term introduced by Marc Horgues, "Metaverse", in *Medium*, published on October 13, 2021, accessed online on November 3, 2021. In the current state of available technological bricks, it is more appropriate to speak of "*miniverses*", according to some specialists.

and others that are partitioned or hybrid. To date, metavers appear to be closed or hybrid at best, despite a few exceptions mentioned below. It is likely that many metavers / minivers will coexist in the future, provided that their interoperability is possible and enables users to move from one virtual universe to another with limited friction. In fact, several digital universes are already offering particularly immersive experiences in 2022[1301] , despite the fact that these online experiences remain mostly centralized and under the control of private companies such as Microsoft, Facebook and Apple. Eventually, the Metaverse will resemble a hybrid of online social experiences, sometimes extended into three dimensions or projected into the physical world. It will make it possible to share immersive experiences with others, either exclusively digitally or phygitally[1302] , enabling people to experience events that are unprecedented or even impossible in the physical world. The Metaverse is a new dimension in human desires and passions. Neal Stephenson's book proposes four foundations for the emergence of a Metaverse that are particularly relevant to the present study:

(i) A reliable, secure *digital infrastructure.* This IT infrastructure involves multiple technologies and consequently a high degree of scalability for each of its technological building blocks. Certain technologies and applications (blockchain, crypto-assets, holograms, sensory sensors, VR and AR headsets) will undoubtedly be called upon to provide an overall infrastructure that is easily accessible, robust, perennial and a source of trust for all stakeholders in this concept. However, bringing together so many technologies and concepts is a major technical and time challenge[1303] . This would be one of the key success factors in moving from a multitude of minivers/metavers to a single Metavers.

(ii) A specific *economic system* and suitable online means of payment are essential to support the functioning and social interactions of a metaverse. The advantages inherent in crypto-assets could be a wise choice for means of payment and value storage[1304] . Some projects such as Decentraland[1305] or The Sandbox[1306] (see below) have already created virtual worlds that incorporate crypto-assets, enabling players to monetize their creations and content, such as casinos and theme parks. Eventually, it will be possible to

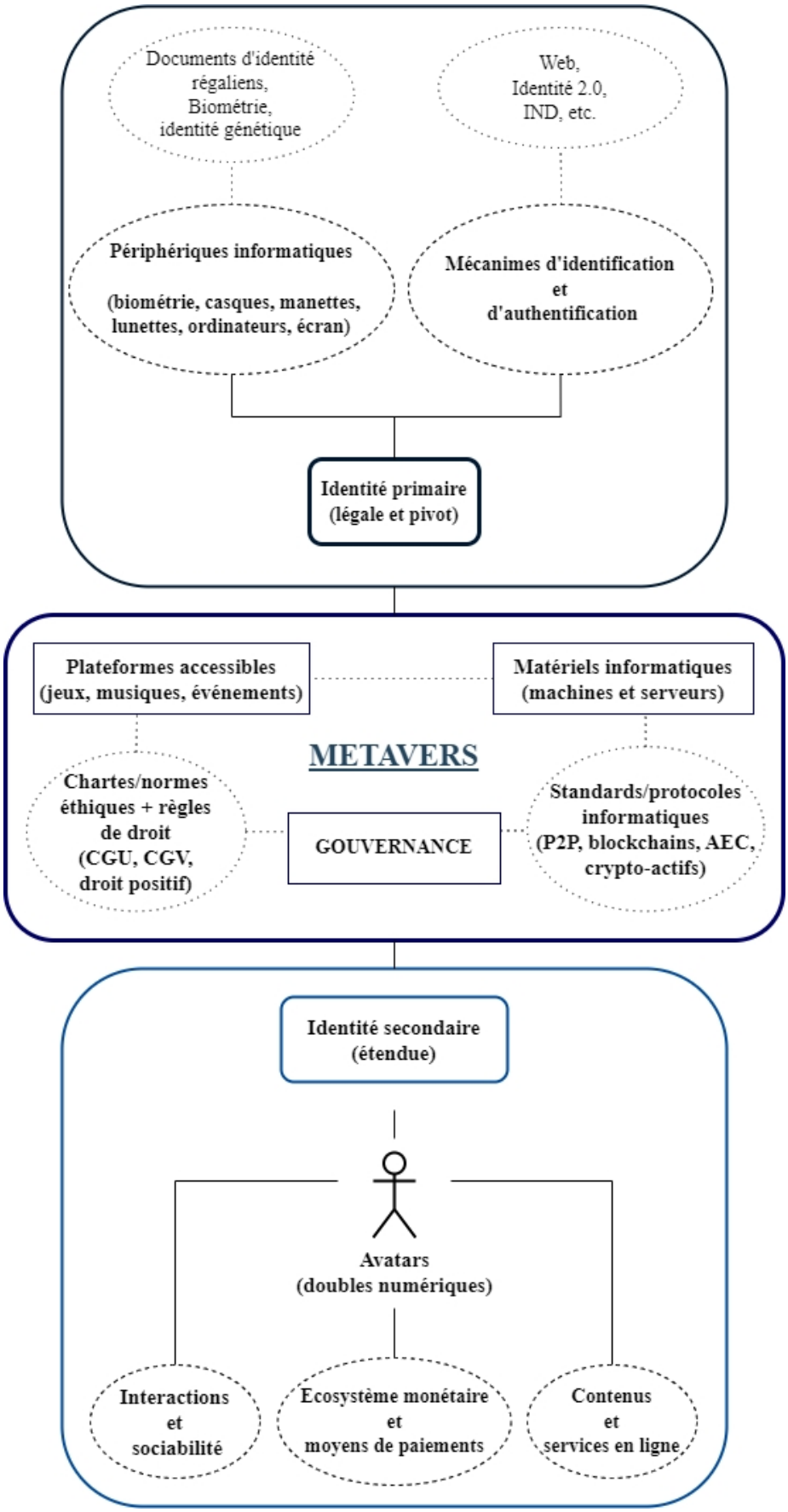
[1301] Non-exhaustive list: *Oculus* or *Hololens* virtual reality headsets for playing video games, pairs of *Ray-Ban Stories* connected glasses for capturing moments in video, series of live music events with over 12.3 million players on the *Fortine* video game platform in April 2021 (containment periods), etc.
[1302] Virtual projection of our physical bodies within a metaverse, thanks to immersive technologies (VR, MR, etc.). [1303] Today, the man-machine interface, i.e. the classic trio of mouse, screen and keyboard, remains a barrier to the user's total immersion in the Internet.
[1304] V. Appendices 3 and 6, Focus 1.
[1305] For more information, visit www.decentraland.org or a similar project www.cryptovoxels.com
[1306] For more information, visit www.sandbox.game

It will be possible to buy and sell virtual goods from different games and universes on interoperable marketplaces, and then move around with your avatars in a more or less immersive way. Crypto-assets could thus become central cryptocurrencies[1307] for Metaverse users. All virtual and immaterial objects would be expressed in crypto-assets, generating intense competition to capture the interaction and value associated with these exchanges. All this would contribute to the realization of the Metaverse's promise to merge several universes into one.

(iii) *Avatars* are needed to extend people's identities within these multiple digital experiences and ecosystems, which will be split up at first and eventually brought together. The use of avatars enables a degree of expressiveness and interactivity close to the real thing, even beyond what is possible today. Nevertheless, these avatars currently only reflect an extended digital version of people's real identities. Yet Metavers could transform the 2.0 digital identities we use today. Thanks to their avatars, users will be able to create and modify certain extended attributes of their identity, plunging them into new possibilities for asserting their identity, in the same way that social networks, for example, have transformed our freedom of expression. Thanks to decentralized, civil, pseudo-anonymous or anonymous identities, users could gradually live a second digital life, working and consuming in a universe that aspires to supposedly limitless creativity.

(iv) The digital micro-companies that Metavers would form would need to reach a *minimum threshold of users* and players to ensure their operation and sustainability, particularly financially. The success of the Metaverse thus seems to depend on its social and digital openness: the more open the ecosystem, the greater the number of services and users that will be able to interface with it, especially as regards the communities of developers who are directly financially incentivized to contribute to and participate in these new phygital, 2.0 and 3.0 ecosystems.

[1307] See *infra*, II, Title 2, 2.4



The diagram above represents the theoretical functioning of a Metaverse and its relationship to digital identity. It was inspired by Matthew Ball's work in 2021[1308] and helps us to understand how people's identity bricks will interact with this ultra-interactive digital ecosystem. To simplify its understanding, a person's identity can be split, as mentioned earlier in this research, into two parts: the primary identity and the secondary identity[1309] . In theory, the Metaverse implies a merged use of all our identity elements, whether root or extended. The secondary identity must be under the control of the user, and the primary identity from which it derives must remain under the protection of a public authority and the rule of law. The aim is to prevent the centralization of Internet users' primary and secondary identities from being orchestrated, in particular, by the companies behind these Metavers (GAFAM/BHATX). Decentralization of digital avatars in a Metaverse thus appears to be as much a technical necessity as a social one, in particular to avoid alienation or dependency of individuals with regard to their digital identity. Responsibility for managing such digital avatars could also lie with the individuals who hold them, and not with a centralizing third party. With regard to the root and pivot identity shown in this diagram, apart from the use of self-sovereign identities (INAS) studied in the previous section of this study, decentralized identity will probably be derived from the civil attributes of individuals and their rights, which implies the intervention of the State and its institutions. If the Metaverse revolution could be as important as the invention of the Internet itself, being in reality in its computer continuity, it will not necessarily be instantaneous and massive as some may think. Growth will probably be slow, gradual and structural, taking only a few decades for a multitude of products, services and dedicated technologies to be integrated and forged. In the meantime, it is possible to anticipate some of its impacts, as the Metaverse introduces a real paradigm shift for Internet users and their social interactions, particularly at work. It could also transform the very concept of citizenship, providing access to new memberships and communities with just a few clicks. This possible competition of citizenships could add to a movement to redefine people's physical and digital identities (*see* Appendix 4).

Today, Metavers is just a utopian idea that is seeing its first forms and expressions. Decentraland, created in 2015, is a decentralized video game platform that operates in P2P to host data, as well as NFTs and a CAD to enhance certain elements of its virtual environment and set up a supposedly decentralized online governance. Users can carry out a variety of virtual interactions, such as purchasing plots of land

[1308] BALL Matthew, "Framework for the Metaverse", in *MatthewBall.vc*, accessed online November 3, 2021.
[1309] See *above*, I, Title 1, 1.2

[1310] , the sale of virtual objects and works of art[1311] , music tracks, etc. Management of the virtual universe is partially decentralized through the use of a dedicated crypto-asset as a means of payment and voting[1312] , combined with a DAO[1313] . For its part, *The Sandbox* is a Metaverse in which players can play, build, own and monetize virtual experiences, offering artists, creators and gamers the means to unleash their creativity. In 2021, Facebook, renamed "*Meta*"[1314] , announced its intention to invest heavily in the concept of Metavers, signalling its interest in this promising sector[1315] and although it is AI that seems to have recently been favoured by the firm in early 2023. By 2026, however, the company plans to offer its own Metavers to its two billion users[1316] . Although it is intuitively possible to think that Mark Zuckerberg's vision for Meta[1317] could differ greatly from the open, interoperable vision formulated by the blockchain industry[1318] , Meta's CTO Andrew Bosworth seems rather optimistic about the openness of the ecosystem and technologies Meta could use, particularly concerning blockchain and crypto-assets, moreover partially implemented in 2022 (avatars on Facebook, NFT on Instagram[1319]). It will probably be necessary to use decentralized identity portfolios (PIND), whether or not they are labeled in the sense of eIDAS, either provided or supervised by public authorities or companies, to prove one's primary or secondary identity in the form of digital avatars within this Metaverse. This will make it possible to re-establish the verifiability of a person's pivotal identity within a digital 3.0 society. The use of VCs (verifiable certificates, as a reminder) appears complementary and perhaps more efficient than the use of NFTs and smart contracts in current minivers (mostly video games). VCs are interoperable, which will facilitate decentralized digital identity (VC, DID) in metaverses,

---

[1310] These virtual terrains can be compared to domain names (within a specific game), sometimes (artificially) rare and coveted. Follow the link below to view the land available in this video game. Each player owning a piece of land can then 'build' the virtual environment of their choice on it.

[1311] Decentraland - Marketplace. Visit the JNF/NFT Marketplace at the following address.

[1312] V. Decentraland, in *CoinGecko*, The "Mana" digital token (based on the Ethereum blockchain).

[1313] The CAD for the *Decentraland* project can be accessed at the following address

[1314] GARCIA-MONTERO Célia, "Facebook renames itself Meta to focus on the metaverse", October 29, 2021, in *JDN*, accessed online November 3, 2021, "Right now, our brand is so closely tied to a single product that it can't represent everything we do today, let alone in the future [...]. Over time, I hope we'll be seen as a metaverse company, and I want to anchor our work and identity in what we're striving for." [1315] CASEY Newton, "Mark Zuckerberg is betting Facebook's future on the metaverse", on *The Verge*, published July 22, 2021, accessed online November 3, 2021.

[1316] CLEGG Nick, OLIVAN Javier, Meta executives, "As we begin to bring the metaverse to life, the need for highly specialized engineers is one of Facebook's most urgent priorities", in a press release [1317] For more information, see the Meta website at

[1318] ROSE Janus, "Zuckerberg Meta Endgame Is Monetizing All Human Behavior", 1er November 2021, in *VICE*, Retrieved online, free translation from English, "While the bait and switch is a familiar and unsurprising move for the company formerly known as Facebook, the Meta announcement proves that nothing can stop Zuckerberg's plans to mine every human interaction in the world for data that can then be monetized."

[1319] NILAY Patel, "Meta's Andrew Bosworth on moving Facebook to the metaverse", in *The Verge*, published November 1, 2021, free translation "Instead of having to store it in a database somewhere, which has its own drawbacks, you store it in the blockchain. And it's possible to say, yes, the system can verify that I'm the owner of this object and that I have the right to make copies of it, or sell it, or whatever. So there's an opportunity there. [...] And I'd be very surprised if they weren't one of the things underlying at least some of this. I'm not sure that every part of the metaverse will be supported by Crypto. But I think it's important to support it [...]" accessed online November 3, 2021.

unlike NFTs, which often depend on different blockchains that are not yet interoperable, if at all. Furthermore, VCs are not linked to an economic valuation, unlike NFTs, which often involve this economic dimension. However, it seems important not to financialize the primary digital identity at the risk of falling into economic excesses, such as digital social credit. The neutrality of decentralized identity must therefore be ensured by the rule of law within a metaverse. According to the diagram presented, content creation is one of the main challenges to be met within a metaverse. Given that everything would be designed by a few companies and their developers, it is important to ensure that the content created respects fundamental rights. In this respect, the commercial implications of the Metaverse raise ethical questions about how these virtual universes will be created and managed. The question of intellectual property arises when content is created for use in a Metaverse. It seems important to think about an appropriate legal framework to govern these activities and protect the rights of users, who are first and foremost citizens. Describing precisely what Metavers will look like in a few decades' time would be as difficult as predicting in 1990 what the Internet we use today would look like. Nevertheless, it is possible to draw some outlines of the Metaverse according to three prospective time scenarios:

1) In the short term, Metavers are likely to be mainly online gaming environments, with access centralized and controlled by a few large, dominant and traditional Web 2.0 players such as Meta and Microsoft. In this first possible scenario, the Metaverse would simply represent a more immersive Internet, thanks to the use of virtual or augmented reality headsets or goggles[1320] . In the short to medium term, it is likely that the Metaverse will not replace the physical world, as is all too often assumed, but rather overlap with it in a particularly immersive way.

2) A second hypothesis suggests that, in the medium term, the centralization of Metavers could be an obstacle to their mass adoption and interoperability. If Metaverse users own assets, earn a living and maintain communities in this digital environment, hardware shortages or service interruptions could pose a threat to their livelihoods and even to the social stability of the Metaverse concerned. Web 3.0 could thus contribute to a decentralization of the Metaverse through hybrid systems, such as private and/or hybrid blockchains, and the use of open source codes. These ecosystems will mainly be managed by organizations that advocate an open, interoperable world, but nevertheless have a core team of operators, who will play a key role in the early adoption of these universes[1321] .

[1320] See "Oculus" gaming headsets or "Google Glass" glasses.
[1321] Wikipedia contributors, "Diffusion of innovations", 2021, accessed online November 3, 2021.

3) The third scenario envisages the long-term emergence of Metavers governed by decentralized autonomous organizations (DAOs)[1322] mentioned in the first title of this study, either via smart contracts themselves issued on public blockchains. The use of public blockchains would provide a foundation of resilience and maximum network effect for any Metavers. The example of a sovereign judicial Metaverse that could offer an immersive experience and strong online identification to deliver online justice would seem less utopian (Kleros for example, already cited)[1323] . This research notes that to be truly immersive, the Metavers concept must use the biometrics of its users, which poses an ethical question for Man and his relationship to the machine. Although many challenges remain, justice will one day have to face up to these new interwoven technologies.

The legal issues involved in a Metaverse are likely to be numerous if it were to take off quickly. Insofar as, for example, crypto-assets represent a new economic incentive for users, even if they avoid the legal and political drawbacks associated with traditional and sovereign currencies, a decentralized Metaverse must not overly modify people's behavior and social perceptions. In other words, the lure of profit, immersion and possible interactivity within the Metaverse must not be to the detriment of the individual and, in the broadest sense, his or her identity. The question of copyright arises, as does the creation of avatars in the Metaverse by celebrities without their consent, as ruled by the Tribunal de Grande Instance de Paris in 2016 in the Polnareff case[1324] , even though this was a television advertisement, but which could well be transposed to the Metaverse. The latter won the case for the use of a lookalike in an on-screen advertisement produced on the initiative of the Cetelem company. Metavers' virtual plots of land, fuelled by artificial scarcity rather than real, physical scarcity, also raise questions about the legal recognition of these plots and the intervention of notaries to secure their exchange and guarantee the success of such sales, which are already topical. It is also important to guarantee the confidentiality of the information exchanged. In 2022, protests were reported within certain video games and Metavers, raising the question of how such events can be framed in a decentralized environment in which there is no policing, nor control by the creator of digital environments. The players currently involved in the development of Metavers should direct their ambitions towards the creation of distributed, sovereign Metavers. To achieve this, public intervention would be needed to fund research in this field and guarantee the protection of Metavers users' privacy, freedom o f expression and data, as China already seems to be doing.

[1322] V. Appendix 9.
[1323] See *supra*, I, Title 2, 2.7.2.
[1324] TGI de Paris, 17th ch. presse civile, June 22, 2016, N° RG : 15/05541.

prepare[1325] . In 2022, Margrethe Vestager announced that the EU was considering a regulation on a possible Metavers[1326] (which raises the question of this definition), and in October of the same year, a report on the development of Metavers was presented in France to Madame Rima Abdul Malak, Minister of Culture and Monsieur Jean-Michel Barrot, Minister Delegate in charge of the Digital Transition and Telecommunications, an essential step in better understanding this concept and its various implications[1327] . The book "*Simulacre et Simulation*"[1328] by French philosopher Jean Baudrillard describes how our modern, digital society has been based on simulations of social reality for two decades now, to the point where it has lost touch with reality. Simulacra and simulations, which should have symbolized the real, have exceeded their function by becoming the real itself. Social networks are a simulation of our social ties, and their digital equivalents (likes and shares) are only simulacra, because they are not physical interactions. The Metaverse reinforces these simulacra, and the question is whether they will end up determining our reality. To avoid losing touch with reality, it is important to prioritize a distributed, phygital digital identity, i.e. one that is partly anchored in reality, as it is linked to our primary identity, rather than an entirely digital, self-sovereign identity that could contribute to the simulacra and simulations described by Jean Baudrillard. We therefore need to be careful that the Metaverse does not accentuate this disconnect between reality and simulacra. According to Michio Kaku, American physicist and futurologist, and author of "*The Future of Humanity*"[1329] , man has always sought to prolong his life and improve his living conditions, which can be seen as an unconscious or conscious quest for immortality. The Metaverse, with its technological, social and economic promises, aims to achieve this utopian goal. The development of Metavers could lead us towards a form of digital transhumanism. In any case, it's essential that the Metaverse belongs to everyone, and that everyone can contribute to it in their own way. The concept of an infinite, borderless Metaverse is not yet achievable with today's technologies, but with technological advances such as

[1325] CHENG Evelyn, "Shanghai doubles down on the metaverse by including it in a development plan", December 31, 2022, in *CNBC*. Accessed online January 12, 2022. As an example, the head of the metaverse industry committee of China's state-backed Mobile Communications Association, Du Zhengping, said: "Traditional Chinese Internet businesses first developed, then were regulated. Industries such as metaverse will be regulated as they develop", *see* also BAPTISTA, Eduardo, "A metaverse with Chinese characteristics is a clean and compliant metaverse", 2022, in *Reuters*, accessed online 01/02/2022, free translation from English "The Shanghai Municipal Commission of Economy and Information Technology has declared its wish to integrate metaverse into its five-year development plan for the electronic information industry. The document calls for the application of metavers to be encouraged in areas such as public services, business offices, social entertainment, industrial manufacturing, production security and electronic games."

[1326] VESTAGER Margrethe, "The metaverse is already here. So of course we are starting to analyze what the role of a regulator will be, what the role of our legislator will be," free translation of a statement by Margrethe Vestager at an online event organized by a group of German newspaper publishers, 2022, in *Euronews*, "EU is analyzing the metaverse ahead of possible regulation, says anti-trust chief Margrethe Vestager". Accessed online February 15, 2022.

[1327] BASDEVENT Adrien, FRANCOIS Camille, RONFARD Rémi, "Mission exploratoire sur les Métavers", *op. cit.* available at

[1328] BAUDRILLARD Jean, "Simulacres et simulation", 1981, Ed. Galilée, ISBN2-7196-0210-4 ISSNOIS2-367B, available online at

[1329] KAKU Michio, "The Future of Humanity", 1ère edition, 2019, Ed. DeBoeck.

artificial intelligence or even trinary computing[1330] , the Metaverse could one day come to life to satisfy some of mankind's utopian fantasies.

1.5 Digital identity and genetics 4.0 between opportunity and risk of technological drift

Over the past few decades, Europeans' identity has relied mainly on biometric systems, as mentioned above. However, recent technological and biological advances have paved the way for a new digital and biological identity - phygital - which we suggest as "4.0". Indeed, with the emergence of new gene-editing technologies, it's fair to ask whether the future of our digital identity will be genetic. Today, all digital content is stored on centralized servers, i.e. within interconnected IT infrastructures. Tomorrow, this same content could be stored within synthetic DNA. The aim of this new concept is to respond to a major problem: how can we sustainably store our ever-growing digital information (videos, photos, music) while physical storage media remain limited? At present, one promising method of addressing this concern is to use DNA as a storage medium. This method involves encoding the data to be stored using a dedicated algorithm, then storing it in small metal capsules. The advantage of DNA storage is that it is stable over billions of years, and can be read several hundred years after encoding. As long as medicine is able to study and decode this encapsulated synthetic DNA data, this storage method will be able to endure. In other words, genetic identity
4.0 could one day solve the problem of the technological obsolescence of computer storage studied above. However, the question of interoperability and how to read this data remains a major challenge, and is still in the experimental phase. In the meantime, November 23, 2021 marks a milestone in data storage, as it is now possible to encode data in DNA molecules. As a symbolic illustration of this breakthrough, the Declaration of the Rights of Man and of the Citizen of 1789, as well as the Declaration of the Rights of Woman and of the Citizen drafted by Olympe de Gouges in 1791, have been stored on synthesized DNA fragments[1331] . This disruptive innovation paves the way for new types of data warehouses (data centers) that are supposed to consume less energy and therefore be more respectful of the environment. The French company Biomemory Labs[1332] aims to make this new type of synthetic biology directly accessible within the computer world by merging them, thus creating a new form of encounter between computing and biology. Other companies are also developing technological variants

[1330] See *infra,* II, Title 2, 1.7
[1331] KARAYAN Raphaële, "Les Archives Nationales inaugurent le stockage numérique sur ADN", November 24, 2021, in *UsineDigitale*, consulted on April 25, 2022, at the following address
[1332] For further information, visit www.biomemory-labs.com

and biometrics of this concept close to transhumanism. Genobank[1333] , for example, plans to use blockchain technology to help individuals manage their DNA securely and with respect for their rights. The public EOS blockchain[1334] , which competes with Ethereum's[1335] , would enable DNA management very close to the concept of self-sovereign identity (INAS). If a company like Meta, which possesses millions of pieces of data on individuals (their geolocation, their spending habits, the identification of their friends and family), were to attempt to merge this data with DNA data, what would the consequences be? It's essential to think about any solution in terms of its uses and their proportionality (what risks for what benefits), while applying a precautionary principle right from the design stage of any new 4.0 solution to come. A proactive approach, involving co-construction with legislators, seems essential, as the CNIL has already been proposing in France for many years on other subjects that were just as disruptive at the time (electronic signature, biometrics, blockchains).

1.6 The rise of machine identity (IoT) in the face of timid legal recognition

The widespread presence of connected objects - computers, telephones, watches - is gradually changing our initial perception of the notion of identity. Algorithms and connected objects are expanding the boundaries of identity, previously reserved for people and computer objects. These "*digital artifacts*"[1336] are increasingly integrated and inseparable from the notion of digital identity, due to their increasingly widespread use in the exercise of our identity. In 2016, legal scholar and CNRS and Harvard researcher Primavera de Filippi anticipated that blockchains could be used to manage a wide range of activities, ushering in a new era of interactions between machines and people that could potentially alter the very nature of our relationships with physical goods[1337] . For example, an object connected to a blockchain could enable the implementation of rights and access control systems which, in the event of non-compliance, would allow access to the service or certain functionalities to be deactivated in real time. In 2014, the Alain Bensoussan law firm drew up the first legal doctrine in France on the presumed legal personality of certain digital and intelligent artifacts such as algorithms, robots and autonomous cars. This work, entitled "*AI, Robots, et Droit*"[1338] notes that, although such a legal status has not yet been officially attributed

[1333] For more information, visit www.genobank.io
[1334] For more information, visit www.eos.io
[1335] V. Appendix 6, Focus 2.
[1336] BENSOUSSAN Alain, "L'identité numérique 5.0", *op. cit.*
[1337] De FILIPPI Primavera, "Blockchain and the Law", in *Harvard University Press*, *op. cit.* location 121 on 7004, "Blockchains could [...] be used to manage a growing range of activities, fostering a new era of machine-to-machine and machine-to-person interactions that could potentially change the very nature of our relationships with physical goods."
[1338] BENSOUSSAN Alain, BENSOUSSAN Jeremy, "AI, robots et droit", 2019, in *Lexing*, Technologie avancée et Droit, Ed. Bruylant.

to these artifacts[1339] , it can be partially recognized and demonstrated on the computer level[1340] . In fact, every computerized object possesses unique identification elements (numbered parts, specific programs) which give it a singular capital (not genetic, but computerized) likely to form a specific identity to which rights and obligations could be attached[1341] . Thus, according to this theoretical principle, any digital artefact (program, robot, intelligent object) that acts on behalf of a legal or physical person, acquires its legal personality and becomes de facto an entity legally responsible for its acts - by transposition of art. 1242 of the Civil Code[1342] - in both the virtual and physical worlds. The use of public blockchains (AEC, DAO) to support autonomous systems (AI) will pose ever greater challenges for states and regulators seeking to control, shape or influence the development of these technologies. From a technical point of view, some connected objects equipped with artificial intelligence (AI) algorithms can make logical deductions. However, it's still hard to say whether this is as complex a form of intelligence as that of human beings, or whether it characterizes an emerging form of identity and self-awareness. In practice, human intelligence and confidence, which are the necessary ingredients for the emergence of complex thought and identity, cannot yet be transposed to machines. However, as the Internet of Things (IoT/IoT) develops and devices become increasingly dependent on emerging artificial intelligence, public blockchains could support devices that are both autonomous and self-sufficient. In 2017, history was made when Sophia, a robot designed by Hanson Robotics, became the first robot to achieve full Saudi citizenship. The news was made public at the Future Investment Initiative in Riyadh. During an interview between Sophia and her creator, David Hanson, Sophia questioned her own identity: "*If my mind is different, then am I still Sophia? Or am I still Sophia?*

? "[1343] Although Sophia's analytical and communication capabilities are limited, is it possible to give her a specific identity? More recently, in 2021[1344] , the Australian Federal Court ruled that an artificial intelligence can be considered an inventor in a patent application. It is theoretically possible to attribute certain human capabilities to machines, but in practice, machines remain largely conditioned and dependent on the humans who design and administer them. The reliability of a machine depends exclusively on its supplier or administrator. Thus, it does not seem appropriate to compare a person's root identity with

[1339] *Op. cit.* BENSOUSSAN. Article 1 of the "Charter of Robot Rights" proposes a specific definition of a robot:
"[...] a robot is a machine endowed with artificial intelligence, making autonomous decisions, able to move autonomously in public or private environments and acting in concert with human beings", available at the following address
[1340] *Ibid*: "A robot has its own identity, an identification number and a capital whose sole purpose is to repair any damage it may cause.
[1341] *Ibid.* Art. 6 of the "Robot Bill of Rights" proposes a first nomenclature for the liability of autonomous artifacts or representatives in the event of damage.
[1342] Art. 1242 of the Civil Code: "One is responsible not only for the damage that one causes by one's own act, but also for that which is caused by the act of persons for whom one is responsible, or of things that one has under one's care", accessed online [1343] "Meet Sophia: the first robot declared a citizen by Saudi Arabia", in *The Jakarta Post*. 30, 2017, [Video]. YouTube
[1344] ROSSO Stella, "For the first time, the status of inventor is awarded to an AI", August 4, 2021, in *Siècle Digital*, available at.

that of a connected object. However, it is possible that one day machines will be able to develop their own extended identity, even if for the time being their root identity remains dependent on humans. Finally, Aurélie Jean points out that the notion of the legal personality of robots has been abandoned in the latest European texts on the subject[1345] .

1.7 Web 2.0 and 3.0: opportunities and precautions in the face of quantum computing (5.0)

The constant evolution of new technologies mechanically implies ongoing research to secure these computer systems and their adjacent digital ecosystems. Cryptography is now an integral part of our information systems. It is essential to ensure a form of digital integrity for Internet users and their online identities. Asymmetric cryptography, which underpins the applications discussed throughout this research, is currently considered a reliable encryption method for protecting all types of data[1346] . However, the advent of quantum computers (the "*quantum supremacy*")[1347] could jeopardize the security of certain[1348] public key encryption algorithms used today on a daily basis without us even realizing it[1349] . Although such quantum supremacy is purely theoretical in 2023[1350] , some major technology companies such as IBM and Google foresee such a possibility in the coming decades due to the rapid advances in this new era for computing. Indeed, the development of a new generation of algorithms and so-called "*quantum*" computers[1351] could call into question the security of certain encryption algorithms. In other words, while there are numerous mechanisms and

---

[1345] JEAN Aurélie, "Les algorithmes font-ils la loi?", *op. cit*, "This idea of the legal personality of robots has now disappeared from the latest European texts on the subject", reading position in the book: 37%.

[1346] FLECHET Gregory, "Le chiffrement des messageries passé au crible des sciences sociales", 2020, in *CNRS Le Journal*. Reference is made to the recent scandal concerning the data decryption capabilities (message conversations, voice messages, etc.) of users of *Facebook* (*WhatsApp*) or *Apple* (*iMessage*) and to the rise of (more or less) encrypted messaging services such as *Telegram* or *Signal*. Available at

[1347] Quantum computers can jeopardize all the *asymmetric cryptography* in use today, especially *Elypstic Curve* algorithms (*ECC*, *ECDH*, *ECDSA)*. However, some algorithms will be more resistant (*RSA*) than others (*Elliptic Curve*), because their length is greater and takes longer to calculate even for a quantum computer.

[1348] MAX, "On dit chiffrer, et pas crypter", in *BlogChiffrer.info*. The term "chiffrer" should be preferred to "crypter", because semantics are important in computer science, consulted at the following address

[1349] In computing, every encryption algorithm has an expiration date. Symmetric algorithms such as *AES* and asymmetric hash functions would also be vulnerable to quantum computers (OQ), but not to the same extent as public-key encryption algorithms. Theoretically, it would be possible to maintain a sufficient level of security by doubling the size of the key or *hash function*. For example, for the *AES* algorithm, a *100-bit* key would be sufficient until 2020, but a *128-bit* key would be required to guarantee security beyond that (source: ANSSI). As for the *RSA* algorithm, a *2048-bit* key would be sufficient until 2030, but would need to be increased to *3072 bits* to guarantee security beyond that in the face of quantum computers. If these key sizes are not increased, encryption could theoretically become obsolete and vulnerable to quantum attacks. However, it is important to note that increasing key sizes would only slow down the resolution of keys by quantum computers, without preventing them from decrypting them completely. V. *supra,* I, Title 1, 2.3.1.1.b

[1350] SHOR Peter, renowned American mathematician and author of *Shor's algorithm*, developed in 1994, which demonstrates in mathematical theory the supremacy o f quantum computer algorithms over certain encryption algorithms of our conventional computers. Wikipedia contributors, 2022, biography at [1351] ABRAM Cleo, "Quantum Computers, explained with MKBHD", for more visual information on the state of the art relating to these computers, see the following video, April 4, 2023, [Video]. YouTube.

algorithms for protecting data (encryption) and transmitting it to a recipient capable of retrieving the original data (decryption), these current methods for securing online interactions are not infallible. The decryption of data by a supercomputer[1352] remains possible, but in practice takes a long time to execute in a reasonable timeframe. To illustrate this point, if a conventional computer were to attempt to decrypt data using an asymmetric encryption algorithm, this would require computing power for several decades, making any decryption attempt virtually impossible. Symmetric algorithms are designed in such a way that recovering the private key from the public key involves solving a complex mathematical problem that cannot be achieved in a reasonable time by conventional computers. This means that solving the problem would take centuries without the help of unconventional, i.e. quantum-capable, computers. Although there are already supercomputers capable of decrypting certain algorithms and data (communications, messages, documents), their acquisition and operating costs remain prohibitive for carrying out massive and recurrent decryption actions. In short, asymmetrical cryptography is currently sufficiently robust to guarantee the security of data exchanged on the Internet, but the emergence of quantum computers could call this security into question in the long term (especially for symmetrical cryptography algorithms).

Quantum computing is a branch of computer science that relies on the laws of quantum mechanics to perform operations and calculations on data. Unlike classical computing, which uses "*bits*"[1353] to store information in the form of 0s or 1s, quantum computing uses "*qubits"*. These can represent a 0, a 1 or both simultaneously (three possible states instead of two in current computing). Thanks to this peculiarity, quantum computers are able to perform calculations much faster than conventional computers, making them capable of solving theoretically more complex problems that the latter are unable to handle. As early as 2014, some authors pointed out that these computers represented a major technological advance that could eventually enable those who mastered this technology to dominate the computing market[1354] . In practice, when a quantum computer is faced with a mathematical problem, it does not go through all the possible existing solutions to find a solution, but directly selects the most reliable options

[1352] The differences between a conventional computer and a supercomputer lie in their purposes and data processing capabilities. A conventional computer is designed to perform routine tasks such as surfing the Internet, checking e-mail or producing documents. Supercomputers, on the other hand, are very high-performance computers designed to perform intensive calculations, such as complex simulations, weather forecasting, scientific modeling or massive data analysis. Supercomputers are capable of processing massive amounts of data in record time, thanks to their specialized and very powerful architectures and software.

[1353] Wikipedia contributors, "Bit", "a bit is the minimum amount of information transmitted by a message, and as such is the basic unit of measurement of information in computing", 2022, available at

[1354] BELLANGER Pierre, "La souveraineté numérique", *op. cit*, "The quantum computer is changing the magnitude of the computer age. It will leave in the dust those who do not master its technology. It is the key to the future computing power of nations", location 3033 of 3565.

among all the possibilities that exist and that it knows de facto. In other words, while your conventional computer tries to assemble a puzzle by exploring all possible combinations, the quantum computer already knows all the possible combinations of the puzzle pieces and only has to calculate the fastest way to assemble them. This relatively accurate analogy helps us to better understand the extent of this quantum supremacy over conventional computing. In computing terms, the power and efficiency of quantum computers could be used to decrypt a private key from its public key, thus revealing the data exchanged in the originally encrypted channel. In reality, it should be noted that there are several types of quantum computers with different computing components, such as "*trapped IONS quantum computers*", which means that a race for performance and stability of these different construction methods has already begun since 2018[1355] . For the time being, these trinary computers are only used in complex, mastered environments, which rules out their adoption and commercialization for private individuals for the time being. Google has, however, announced its ambition to provide consumer commercial access to quantum computers by 2029, an ambition that only time can confirm[1356] . The rise of quantum computers in several major world powers, such as the USA, China and Europe[1357] , is also raising concerns about the security of people's physical and digital identities. As IT expert Rémi Fugier, a member of the European professional association Eurosmart, explains: "(...) the *very existence of quantum computers breaking asymmetric cryptography will destroy the trust people have placed in digital signatures and seals. This will have major legal consequences, as all digital documents with legal value* [including identity documents] *will immediately become null and void. The confidentiality of data based on asymmetric cryptography will be compromised*"[1358] . While such cyber-attacks seem theoretical at the moment, the members of the Eurosmart consortium point out that "(...) *these risks may already exist today concerning the digital signature, the digital seal or encrypted data, which can be captured and stored by attackers, with a view to exploiting them in a few decades' time, when quantum computers will be available*"[1359] . If the technology disrupts itself (quantum supremacy), how will legislators react, given the current difficulties they face in grasping certain bricks of conventional computing? If quantum computer technology were to be widely adopted rapidly, society might not

[1355] GAUDIAUT Tristan, "L'infographie entre dans l'ère numérique", 2021, in *Statista Infographies*, consulted online December 1, 2021.
[1356] CASTELLANOS Sara, "Google Aims for Commercial-Grade Quantum Computer by 2029", May 18, 2021, in *The Wall Street Journal*. Retrieved February 15, 2022, from
[1357] Since the publication of a US report in September 2018 on the subject of quantum computers (QCs), a race for quantum computers has been launched on a global scale, v. Report "NSTC National Strategic Overview for Quantum Information Science", accessed online on December 1, 2021.
[1358] EUROSMART Association, Working Group (IN Groupe, Idemia, Thales, et al.), "Quantum computers & identity documents", accessed online November 29, 2021, p.5.
[1359] *Ibid*.

not be able to effectively protect certain rights exercised online, notably the distribution of authorizations and data attributes attached to any online identity. The consequences of this could generate the falsification of access rights and authorizations to certain IT components such as digital signatures, communication channel encryption, data time-stamping or even the impersonation of individuals, according to some legal experts[1360] . However, as with all digital technologies, quantum computing is only a tool for specific use cases. For example, is intellectual property law adapted to quantum computers? To answer this question, a research paper published in 2021[1361] proposes shorter terms of protection (from 3 to 10 years) for intellectual property rights linked to creations and inventions associated with quantum computers (software, hardware, algorithms). This would ensure greater legal certainty, while encouraging the dissemination of knowledge and the monitoring of innovation in this field. Political decision-makers will need to strike a balance between freedom and control for these 5.0 technologies. At this stage, it seems that quantum computers can be seen as a threat as much as an opportunity. The risk of quantum supremacy is regularly questioned, yet the mere possibility of its materialization must be taken seriously. In 2023, the Web 3.0 ecosystem sometimes seems to underestimate this threat, as mathematician Fernàndez-València explains: "(...) *it is important to point out that, despite major initiatives such as the NIST project, no major project focuses exclusively on providing quantum resistance to blockchain.*"[1362] . The difficulty of getting updates accepted on a blockchain, particularly a public one but also a hybrid one, limits the ability of these ecosystems to react quickly in the event of an unexpected quantum attack, although this seems unlikely at present. It is therefore important to continue encouraging research in this field, and not to underestimate this potential threat in the years to come.

As far as the Bitcoin blockchain is concerned[1363] , it seems that quantum computers will not pose a real and serious threat by at least 2030[1364] . On the other hand, in the 2.0 computing ecosystems that have been preparing for the eventual arrival of quantum computers for several years now, the opposite situation can be observed. As a reminder, in order to guarantee an environment of trust for consumers and users of crypto-assets, it is necessary to provide a legal framework for certain financial uses linked to public blockchains. However, this must not be to the detriment of the development of these open ecosystems, i.e. by focusing solely on

---

[1360] BENSOUSSAN Alain, "L'identité numérique 5.0", "Quand les ordinateurs quantiques pourront casser les systèmes de chiffrement à clé publique, ils ne cassont pas que les communications cryptées [chiffrées], mais toutes les identités", *op. cit.* in *Lexing*, p.19.

[1361] KOP Mauritz, "Quantum Computing and Intellectual Property Law," 2021, in *Berkeley technology Law Journal*, Stanford Law School. Vol. 5, available online

[1362] FERNANDEZ-VALENCIA Ramsès, "Post-Quantum Cryptography, a blockchain perspective", 2022, in *Medium.com,* Accessed 05/30/22, available at the following address

[1363] V. Appendix 3.

[1364] GUILLEMET Charles, SERVANT Victor, "Should Crypto Fear Quantum Computing?", 2023, in *Ledger.com*, available at the following address; *see* also the following analysis

irregularities such as money laundering or environmental impact. It is crucial to promote the innovation inherent in public blockchains, as this could lead to the emergence of new algorithms resistant to quantum attacks, thanks to their vast communities of experienced developers. It is therefore important not to pit private and hybrid blockchains against the public blockchains from which they originate, particularly with regard to the potential threat of future quantum supremacy. Indeed, legislating against public blockchains would prevent these ecosystems from finding new technical solutions that private and hybrid blockchains might need through technological trickle-down, given that their developer pools are more limited than those of public blockchains, which benefit from a greater network effect and trust.

In short, quantum computers do not pose a threat to all encrypted data, but mainly to sensitive encrypted data, such as financial, biometric or healthcare data. If the data protected is sensitive for a relatively short period, the quantum risk is negligible. However, if this data remains sensitive for a long period, it is important to take into account certain potential quantum threats, such as the malicious capture of encrypted data for subsequent decryption by quantum computers[1365] . While it is complex to attempt to predict the advent or otherwise of such trinary computing, as cryptologist Jean-Jacques Quisquater points out in 2021[1366] , it does seem crucial that legislators and players in the IT industry, including those involved in digital identity and Web 3.0, take certain potential threats posed by quantum computers seriously. The USA is currently leading the development of "*post-quantum"* industry standards, i.e. resistant to the computing power of conventional and quantum computers[1367] , but it's not too late for Europe to reverse this trend by investing heavily and asserting a strong political will on the subject, as seems to be the case[1368] . Post-quantum algorithms do not require quantum computers, but are simply a new public-key encryption method that is not threatened by quantum computers. Finally

[1365] For example, some entities are already storing primary identity information, encrypted and protected for the time being, but with a view to decrypting it at a later date should quantum supremacy allow it.
[1366] "These words [concerning the potentially devastating effects of quantum computers on conventional cybersecurity] were already being said 10 years ago". Interview with cryptographer and Emeritus Professor of Mathematics Jean-Jacques Quisquater at the International Forum on Cybersecurity (FIC) on 09/09/2021, Round Table:
"What alternative models for identity?
[1367] In 2022, the U.S. National Institute of Standards and Technology (NIST) cybersecurity repository proposed a selection of future standards for quantum power-resistant (post-quantum) cryptography: "These four algorithms [CRYSTALS Kyber, CRYSTAL Dilithium, FALCON, SPHINCS+] will therefore serve as the basis for drafting U.S. federal standards. However, the scope of NIST's announcement is in fact international; this is due not only to the international nature of the competition, in which the cryptography research community is heavily involved, but also to the fact that future American standards will also be used de facto as international industry standards. [...] In the years to come, these post-quantum algorithms will still have to be used in a hybrid mode, i.e. combined with a recognized and proven pre-quantum public key algorithm [...]", "Sélection par le NIST de futurs standards en cryptographie post-quantique", ANSSI, in *ssi.gouv.fr*, available at the following address
[1368] In 2023, a European fund with a budget of one billion euros dedicated to the development of quantum computing has just been announced by the EC, "Building Europe's Digital Future", available at.

On the other hand, it is possible that the economic and digital players in society will preemptively choose to use encryption algorithms resistant to quantum computers in the coming decade, which would drastically limit the risk of this supposed quantum supremacy, which for the time being remains totally theoretical and utopian. 3.0 technologies therefore seem out of reach in the short to medium term, as quantum computers are officially developed to revolutionize sectors such as physics and mathematics.

1.8 Legal, social and IT recommendations for a 3.0 identity

1.8.1 Structural and complementary proposals

In the light of the information gathered and developed in this study, it would appear that a number of recommendations are desirable in order to avoid abuses or negative aspects relating to 3.0 technologies, but also to promote their positive aspects. To this end, the following summary table is proposed:

Complementary proposals (PC) and structural proposals (PS)
PC n°1: It is suggested that a common French-language semantic be created for possible translations and definitions of key decentralized identity terms (VC, VP, DID), from English into French. This would enable lawyers or legislators to use this glossary. Furthermore, in line with the CNIL's personal data protection requirements, decentralized identity solutions should be able to communicate their data protection benefits clearly and easily[1369] . **PC n°2:** In 2017, legal scholar Yves Bismuth proposed the introduction into French law of the concept of "[1370] . In his view, this would oblige the public authorities to set up a legal shield to protect all Internet users, enabling them to surf freely and in complete serenity. Although this vision could be considered utopian in view of the scale and current functioning of the Web, it seems necessary in view of the current general situation of digital plunder and the lack of knowledge and education of Internet users in this area, as this research shows. This concept could also be articulated with the concepts of informational self-determination or digital integrity mentioned in the previous title of this study. **PC n°3:** Draw up a European Charter of best practices for the IND and, more broadly, for Web 3.0 and its various technological bricks. In consultation with identity providers, online services and collective management organizations, such a Charter would aim to to establish a moral obligation of transparency for 2.0 and/or 3.0 algorithms.

[1369] LAHLOU Névine, "Les enjeux de la communication claire appliquée à la protection des données", in *LINC*, 2021, available at linc.cnil.fr

[1370] BISMUTH Yves, "Le droit de l'informatique", 4th edition, 2017, "It could be proposed to introduce, at least in French law, a kind of notion of peaceful enjoyment of the internet".

It should be noted that this Charter would be complementary to the "*codes of conduct*"[1371] set out in eIDAS-2 concerning PINDs relating to the digital identity of European citizens. It is essential that developers of distributed 3.0 solutions take ethical and legal considerations into account in their daily contributions, just like lawyers for whom deontology and the notion of responsibility are a priori omnipresent by design. Consequently, the IND should offer a high level of long-term trust, avoiding the use of unique persistent identifiers and favoring instead the use of temporary and 'disposable' identifiers where appropriate (to avoid the risk of re-identification). It is also important that decentralized identities minimize digital credentials to avoid users feeling digitally overwhelmed by too many of these 3.0 attributes. In addition, decisions should not be made solely on the basis of computer data processing, which means that official physical credentials should be used in the event of doubt or incident concerning a person's digital identity. It is also important that minorities, disabled people and people excluded from the digital world can be taken into account and included through acceptance of such a Charter. Finally, full transparency of an IND's value chain should be a fundamental principle of any 3.0 solution, to generate maximum digital trust while minimizing the risks of altering people's identities.

PC #4: Regarding the smart contracts (AECs) as well as decentralized autonomous organizations (DAOs) studied, our research confirms three of the recommendations published in September 2021 by the European Commission in a dedicated report[1372] : (i) Europe-wide qualification and legal recognition are needed to exploit the potential of these distributed applications and to frame their use as a contractually valid IT mechanism for the automated exchange of consents (leading to a reinforced presumption of data and identity integrity) ; (ii) support technical solutions that enable computer code to be translated into natural language and vice versa (Ricardian contracts)[1373] ; (iii) establish data units within European and national courts or regulatory agencies with technical expertise in AEC and blockchain registries[1374] (or even INDs). As far as DAOs are concerned, legislators could study, take up and draw inspiration from the legislation put in place by the State of Wyoming[1375] .

[1371] Proposal for a Regulation (EU) of the Parliament and of the Council amending Regulation (EU) No 910/2014 as regards the establishment of a European framework for a digital identity, *see* Recital (28) and Section III, art. 12b, 4. Available at.
[1372] SCHREPEL Thibault, "Smart contracts and the digital single market through the lens of a 'Law + Technology' approach, A report for the European commission on smart contracts", CE, 2021, in *NetworkLawReview.org*, pp.57-58.
[1373] *Ibid*. Proposal no. 16 of the Report.
[1374] *Ibid*. Proposal no. 8 of the Report.
[1375] In Wyoming, a DAO is a limited liability company with special provisions allowing the company to be algorithmically directed or managed via smart contracts (wholly or partially). Applicable since March 2022, this law creates a supplement to the Wyoming Limited Liability Company Act to provide a law controlling the creation and management of a DAO. In principle, the provisions of the Limited Liability Company Act apply to a DAO. This law establishes basic requirements for member-managed or algorithm-managed DAOs and provides definitions and regulations for DAO formation, articles of organization, operating agreements, smart contracts, management, standards of conduct, member interests, voting rights, member withdrawal and dissolution of a DAO. See "Enrolled act no. 73, senate sixty-sixth legislature of the state of wyoming 2021 general session", available online; *see* "Decentralized Autonomous Organization (DAO) FAQ", available online.

PS No. 1: First and foremost, we advocate the implementation of a wide range of education and training initiatives[1376] , tailored to the specific needs of different audiences[1377] , in order to better understand the benefits and limitations of IND as well as blockchain technologies and technology bricks mentioned throughout this study.

PS No. 2: It is imperative to design right now a national vision and strategy for IND that is both compliant with EU law (eIDAS-2, RGPD, TFR, DMA/DSA) and conducive to disruptive innovations (public blockchains, ZKP, DAO, Layer 2[1378] , etc.). This strategy should be implemented by systematically using *sandbox regulations* to enable contextualized, relaxed and co-constructed experimentation - by public and private spheres - in the field. To achieve this, multilateral agreements and partnerships should be established between the private and public sectors, subject to strict specification requirements, which is what the Alliance Blockchain France has been proposing as an illustration since 2021. Legal scholar and University Professor Yves Poullet argues that it is necessary to promote better collaboration between the State, which is the guarantor of citizens' primary identity, and private companies, which may legitimately require facilitated electronic access to civil registry data (RNIPP, RNE, etc.) in certain cases[1379] .

PS No. 3: Regarding the use of blockchain technologies for digital identity solutions, this study argues that none of these technologies should be ruled out in the long term, as was emphasized in 2020 in an information report by the French National Assembly[1380] , including public ones that are certainly not compliant with current law (RGPD/eIDAS), as they could become so by implementing second-layer solutions as studied in the Annexes. It is also argued that not all self-sovereign digital identity solutions (INAS) benefit from technological neutrality[1381] although favoring regal digital identity 3.0 solutions seems more relevant in the short term. It should be remembered that regalian 3.0 digital identity solutions are distributed and not decentralized, i.e. they will be guaranteed by the State, its institutions or certified companies.

PS n°4: Given the current climate and societal challenges, it seems essential to encourage institutional work on the environmental footprint of blockchains in the context of IND and INAS development. Once these analyses have been objectively confirmed within a pragmatic timeframe (rather than the short timeframe currently favored), we need to strengthen public support for the most viable IND solutions i n terms of

[1376] MAGNIER Véronique, "Today, companies don't necessarily have all the possible applications of blockchain in mind. People need to be trained to understand this technology and master it", remarks by the Professor of Law, in *L'Édition de l'université paris-saclay*, Summer 2021, n° 16, p.10.
[1377] EC, "Communication Shaping Europes Digital Future", *op. cit,* "Digital literacy and skills have become a prerequisite for effective participation in today's society", accessed online December 6, 2021, p.4.
[1378] V. Appendix 3.
[1379] EYNARD Jessica, CASTETS-RENARD Céline, GUINAMANT Ludovic, "L'identité numérique; quelle définition pour quelle protection?", *op. cit,* "Plaider pour une meilleure collaboration entre l'État, garant de l'identité civile les entreprises privées, qui revendique de manière légitime l'accès électronique et facile aux données du registre de l'état civil", p.205.
[1380] KARAMANLI Marietta, HENNION Christine, MIS Jean-Michel, Rapport d'Information n°3190 sur l'identité numérique, Assemblée nationale, "Le recours à la blockchain pourrait néanmoins être écarté en matière d'identité numérique des mineurs s'il s'avérait que cette technologie ne peut pas garantir avec certitude le droit à l'oubli ou à l'effacement des données", consulted online on August 9, 2021.
[1381] *Ibid,* "Recommendation 40: Encourage the development of alternatives to regalian digital identity, such as self-sovereign digital identity, by exploiting the possibilities offered by blockchain", p.109.

energy. This observation also seems valid for certain public blockchains such as Bitcoin according to Appendix 6 of the present study[1382] .

PS n°5 : Finally, in a January 2022 report[1383] , the Conseil National du Numérique (CNNum) recommends 12 political, legal and social levers for debating new online rights and obligations. Some of these recommendations are perfectly in line with IND's need for guidance and support, such as proposal no. 3: *"3. Recognition of a right to parameterize content and transmitters* [right to INAS]". The aim would be to offer Internet users a new possibility of self-determination regarding the perimeter of the data they decide to communicate according to their digital behaviors, of which they would finally become the sole technical owners. The CNNum also recommends "*6. The creation of a right to interoperability between platforms*.
" 8. Strengthen critical and practical education in digital media as part of school and extracurricular projects" and "*12. Support, design and develop new digital practices and devices that strengthen joint attention and social ties without reducing individuals to impulsive behaviors or cognitive mechanisms*". In addition to the aforementioned recommendations, which are in line with the conclusions of this study, a second report published the same year by the French Ministry of the Interior, and rightly dedicated to the IND, leads us to support the emergence of four new digital rights for Internet users: "[i] *Right to the preservation of a space of intimacy that concerns all the individual's personal data, whether or not they allow him or her to be identified by name;* [ii] *Right to "digital security*
"iii*] The right to resilience of digitized legal identity in the event of an attack;* [iv] *The right to benefit from a trusted digital environment, where legal security is preserved and where the claims made can be proven and/or certified, thanks to the deepening of the relationship between the State and other key players in the life of the citizen (banks, insurance companies, educational establishments, etc.).)*"[1384] . Taken together, these eight recommendations represent structural political, legal and IT levers at the service of a new digital identity 3.0.

PS n°6: As a consequence of the recent interest in artificial intelligence (AI), IND standards would enable the industrial implementation of decentralized identifiers and unique cryptographic signatures to certify the originality and source of any content published online. This is necessary if the origin of such content is to be verifiable, thanks to digital proof 3.0, thus guaranteeing its integrity and promoting the responsibility associated with publishing content online. However, such transparency needs to be studied on a case-by-case basis for each situation and online service, to avoid any misappropriation of purpose such as systematic, mass identification to the detriment of a right to online pseudo-anonymity.

[1382] V. Appendix 6, Focus 1.
[1383] Conseil National du Numérique report, 2022, "Your attention, please! Quels leviers face à l'économie de l'attention?". Available at the following address
[1384] *Op. cit,* COUTOR Sophie, HENNEBERT Christine, FAHER Mourad, "Blockchain et identification numérique, restitution des ateliers du groupe de travail 'blockchain et identité' (BCID)", consulted online, p.49.

Chapter 2: Analysis of practical cases involving cryptographic identity or rights 3.0

2.1 3.0 legal proof of existence for children without identity with DID4ALL

To a certain extent, blockchain technology tends towards universality of exchange, enabling anyone, regardless of origin, skin color, culture or nationality, to benefit from the advantages of these solutions without being discriminated against by these 3.0 protocols. In principle, all users are supposed to be equal before decentralized protocols. Open blockchains have succeeded in creating true universality of (crypto)financial services, offering a universal alternative where public institutions have sometimes failed. However, decentralization can be a myth confronted with physical, software and social reality[1385] . This section aims to compare the *Proof of Humanity (PoH)*[1386] system, which is particularly decentralized to combat censorship, with the "DID4ALL" project initiated in 2019 by the IN Groupe company to provide a decentralized identity that complies with positive law[1387] . The DID4ALL project aims to set up and guarantee a regionalized, inclusive, reliable and sustainable registration system at the service of the life course of children who have no legal existence in their country. According to UNICEF, this situation affects over 166 million children worldwide. The aim of DID4ALL is to test a digital 2.0 and/or 3.0 solution in developing countries, using three technologies that can be combined: (i) voice recognition (by telephone), (ii) an open or closed blockchain and (iii) telecommunication systems (SMS). This solution provides each child with a cryptographic, dematerialized proof of existence that is legally valid throughout his or her childhood. This proof of existence can, for example, be easily deployed by UNICEF, without the need for Internet access for the children and adults concerned in the field. It is therefore accessible to all, including those who cannot read or write. It is reliable thanks to voice identification, which constitutes a unique and secure authentication factor due to the data stored in a distributed manner (P2P). This cryptographic proof of existence is time-stamped on a public, private or hybrid blockchain, depending on the specific situation of each state requesting this solution (due to their infrastructures). The DID4ALL project aims to answer the following question: can a universal proof of existence on blockchain remedy statelessness, which is defined by international law as "*a person whom no State considers to be its national in application of its legislation*"?[1388] This project is scalable and can use multiple technological variants to provide a proof of existence - completely decentralized or distributed if necessary - to miners (and adults) without an identity or means of proving it.

[1385] V, Appendix 7.
[1386] V. *supra,* II, Title 1, 2.9
[1387] DID4ALL by IN Groupe, "Use case: proof of existence for children without identities", available at p.50. See also Margo's November 12, 2019 video for the Blockchain Hackathon for UNICEF, available on YouTube
[1388] UNHCR, "What is statelessness?", in *The UN Refugee Agency*, available at

due to limited or non-existent state infrastructures. The following table therefore compares the PoH solution with the advantages of the DID4ALL solution, which is hybrid (distributed) IT, i.e. compliant by design with the texts and positive law of the legal systems concerned:

Key success factors (KSF) for DID4ALL	**Short term**	**Medium-term**	**Long term**
Legal and political recognition	□ or ~	□	□
Social adoption	□	□	□
Computer adoption and recognition (open or closed blockchain, SMS, voice recognition)	□ or ~	□	□

This table suggests that the key success factors of a legally compliant distributed digital identity drastically increase its probability of success, i.e. adoption in the field. More specifically, it should be added that it is vital to protect the privacy of minors when they use online services, including state services, which DID4ALL enables in comparison with the *Proof of Humanity (PoH)* system. It is customary for service providers to implement a reliable procedure for verifying the age of users in order to determine the limits applicable to data collection. In accordance with Article 8 of the RGPD, a data controller must obtain the consent of individuals before processing their personal data. In some countries where the RGPD does not apply, digital consent can be given from the age of 13. However, under our positive law, a minor cannot give consent alone. Consequently, the data controller must verify the minor's age. To obtain such informed consent, the data controller must explain clearly and simply the use that will be made of the personal data collected. In developing countries, such legal principles to protect individuals are not always provided for, nevertheless, it seems important that European digital service providers ensure they offer such minimum legal guarantees.

2.2 Decentralized identity for Bitcoin with the ION protocol

In March 2021[1389] , after a decade of research and development in the field of decentralized digital identity, Microsoft announced the launch of an experiment and a new protocol called "*Identity Overlay Network - ION*"[1390] . Also supported by the Decentralized Identity Foundation (DIF), this network aims to facilitate the exchange of decentralized identifiers (DIDs) issued by identity providers or Internet users, directly via the Bitcoin blockchain studied in Appendix 3[1391] . According to Microsoft, a network of decentralized identifiers must meet several key requirements, including being open and permissionless, being accessible worldwide and producing verifiable records for all involved. This is why Microsoft has chosen to build this open-source protocol[1392] on the Bitcoin blockchain. It meets all these requirements. This decision to link the ION protocol to the public Bitcoin blockchain is both a strategic choice and a political gamble on the future, as this study demonstrates. This decision was taken because of the security of the Bitcoin blockchain, which is both secure and independent, as it belongs to no one yet is accessible to all. In concrete terms, the ION protocol is a P2P computer protocol for the creation and verification of decentralized identifiers (DIDs). It is a public, distributed and permissionless second-layer (L2) network, which means it aims to achieve a high degree of decentralization, like the Bitcoin blockchain on which it is based. No company, organization or group controls the credentials stored in the ION system, and no one dictates who can participate (not even Microsoft). The Bitcoin blockchain has its own graphical interfaces summarizing transactions on its network[1393] and the ION protocol also has its own interface[1394] , so these two interfaces are articulated together in a complementary way to facilitate the interaction of digital identities (DIDs). Technically, transactions and events involving digital identifiers anchored on the ION protocol are incensurable and immutable thanks to the Bitcoin blockchain[1395] . Microsoft's ION team has stated that "*Bitcoin is so superior to all other* [blockchain] *options, there's not even a comparison - Bitcoin is the most secure option with an absurd margin* [of error]. *It offers a secure alternative to usernames and passwords.*"[1396] . The main value proposition of the ION protocol is its ability to aggregate tens of thousands of decentralized identifier operations into a single

[1389] DINGLE Pamela, "ION, We Have Liftoff!", May 25, 2021, in *Techcommunity.microsoft.com*. Retrieved April 5, 2022, from
[1390] For further information, visit the following website
[1391] V. Appendix 3, Focus 1 to 6.
[1392] The code for this program is licensed under the Apache 2 License, W3C Intellectual Property terms, and the content is available under a Creative Commons 4 Attribution license.
[1393] For further information, visit www.mempool.space/fr
[1394] For further information, visit www.identity.foundation/ion/explorer
[1395] In other words, the ION protocol depends on the Bitcoin protocol to function, but the Bitcoin blockchain can function without the ION protocol. Note that the P2P nature of ION is partly inspired by the Lightning Network. [1396] "Microsoft ion bitcoin", 2021, in *Goldfasanblog,* at

Bitcoin transaction[1397] , which considerably increases the network's volume (as mentioned in Part 1). Microsoft's strategy for the ION infrastructure is to offer an open, robust and secure network (enabling network effects and economies of scale), while overlaying some of its private services such as Microsoft Azure[1398] , which in turn is a source of positive externalities for the company and its 2.0/3.0 application ecosystem. In this vein, Microsoft has also announced the launch in 2022 of a new IND software solution, called "*Entra Verified ID*"[1399] , which can operate either with or without ION and therefore blockchain. It is important to emphasize that Microsoft is not seeking to encourage the tokenization of individuals' digital identities (i.e., by linking people's identities to bitcoins), but rather to provide verifiable identifiers under the direct control of individuals (self-sovereign identity) or trusted entities (computer-distributed identity, i.e., hybrid). The ION protocol appears to comply with legal requirements for the confidentiality of individuals' personal data in accordance with the RGPD. Each of these parties retains ownership of all elements of its identity[1400] . However, it is unlikely that any government will use a bitcoin-related service in the short to medium term, due to the negative image associated with this blockchain in the minds of most public institutions (more or less proven fears of money laundering, terrorist financing or high energy consumption as previously studied[1401]). Consequently, although the ION protocol seems technically and economically suited to INAS solutions, its use for distributed and governmental identities remains subject to political and governmental acceptance. In 2023, the ION network is still at an experimental stage, and has a number of limitations to consider. For an identity provider to use the ION protocol, it must lock in around 0.66 bitcoins, or around 17 euro cents per transaction in early 2023, so that transactions of 1,000 operations can be accepted by this protocol[1402] . What's more, anchoring decentralized identifiers can take up to 20 minutes, which may not be fast enough for certain industrial use cases requiring a digital identity. ION has the merit of demonstrating that the Bitcoin blockchain will probably be dedicated to other use cases as its IT development progresses, as described in Appendices[1403] .

[1397] ION can integrate *10,000* identification *operations* into a single transaction (containing proofs of identity) on the public Bitcoin blockchain

[1398] In other words, if Microsoft initiated and makes freely available the ION protocol (everyone can contribute to the network) Microsoft also proposes and promotes its own IND services such as "Azure active directory verified Credentials service", *v.* "Introduction to azure active directory verifiable credentials (preview)", in *Microsoft Docs*. Accessed April 5, 2022, at the following address

[1399] PATEL Ankur, "Microsoft Entra Verified ID now generally available", 2022. Available at

[1400] Free translation from English, "DID IONs can only be deactivated by their owners, protecting people from digital rights violations", visit www.identity.foundation/ion

[1401] V. Appendix 6, Focus 1.

[1402] For more technical information on this protocol, visit the following GitHub site.

[1403] V. Appendix 3, Focus 3, 4 and 6.

2.3 Self-sovereign identity for crypto-assets with the tbDEX protocol

In November 2021, Twitter founder Jack Dorsey announced the launch of a new project called tbDEX[1404] , via the company TBD[1405] , itself funded by his recent startup Square[1406] . This project also aims to host self-sovereign identities (INAS) using the Bitcoin blockchain as a registry for identity attribute transactions. More specifically, the tbDEX protocol will be a distributed computing infrastructure (P2P) enabling users to buy and sell bitcoins, and possibly other crypto-assets over a long period of time. It will be an online service and protocol similar to a crypto-asset platform or exchange, but decentralized. The aim of this protocol is to provide superior trust and execution speed to centralized exchange platforms, while guaranteeing a maximum degree of decentralization for its users, and complying with international regulations[1407] . TbDEX aims to become a new, decentralized and trusted intermediary, ultimately offering an innovative alternative that is universally accessible and resistant to IT and financial censorship. The tbDEX project introduces the term "*Web 5.0*"[1408] in its online communications, in reference to the Web 1.0, 2.0 and 3.0 generations previously studied, but above all in reference to the programming language
"HTML5 is now ubiquitous on the Internet[1409] . The launch of the tbDEX platform is scheduled for the end of 2023. Although theoretically no personal user information is directly collected by this protocol, it is necessary for certain entities involved in the process (financial institutions, natural or legal persons offering exchange services) to carry out prior identification with different levels of guarantee within the meaning of the eIDAS Regulation, such as low, substantial or high[1410] . Once the user has registered (via a KYC) with one of these third parties designated by the protocol as a "*Participating Financial Institution - PFI*"[1411] , he or she will be able to authenticate themselves autonomously and securely within the entire ecosystem set up by tbDEX thanks to the decentralized identity standards we have studied (P2P, PIND, VC, DID, ZKP, electronic signature). This new protocol will enable legal entities to benefit from

[1404] "tbDEX: A Liquidity Protocol v0.1". Access to the open source code for this protocol is available on the project's Github (below). The White Paper presenting the project is also being revised by the community and is available at the following address
[1405] TBD's first bitcoin-focused product will be *tbDEX*, a decentralized exchange platform that acts as a liquidity protocol for the P2P buying and selling of bitcoins.
[1406] Société Square, *see* following website
[1407] "However, the information required may vary depending on the jurisdiction", p. 7 of 18, and see *supra*, I, Title 2, 2.5.
[1408] "Web5: an extra decentralized web platform", 2022, in *TBD*, available at
[1409] TBD, "Are We Web5 Yet?", free translation from English, "The term Web5 is a throwback that pays homage to HTML5, which was used to represent the last major effort to evolve the Web some fifteen years ago.", available at.
[1410] *Op. cit.* White Paper tbDEX, "PFIs [...] may be subject to different rules and regulations for fiat currency payments, depending on their specific jurisdiction, they are likely to need to collect certain personally identifiable information (PII) from portfolio owners in order to meet regulatory requirements, such as compliance with anti-money laundering (AML) programs, combating the financing of terrorism and non-violation of sanctions.", p.6, *see* also *supra,* II, Title 1, 2.1.1.1
[1411] *Op. cit.* tbDEX White Paper, "Participating Financial Institutions (PFIs) are entities that offer liquidity services on the tbDEX network", p.6.

advantages of a decentralized or distributed digital identity, which will also benefit their users, who will then be able to manage and administer their own verified credentials (as with an INAS)[1412] . As a result, tbDEX will offer both distributed and self-sovereign digital identities, the boundary between the two being as yet unclear for this new system and concept within Web 3.0. Each PIND user will be able to generate his or her own self-sovereign digital identity by going through a reputation-based certification process, which will be evaluated by electronic peer-to-peer social recognition mechanisms (such as the operation of more or less reliable certified reviews on certain online services, such as the TripAdvisor online service). In addition, to guarantee user identification and authentication on this new protocol, it is highly likely that PFIs will resort to specialized services offered by companies with expertise in analyzing and combating illegal transactions carried out in crypto-assets (Chainalysis or CypherTrace)[1413] . Although this protocol aims in principle to maintain a certain technological neutrality[1414] , it nevertheless tends to offer its users a right to pseudo-anonymity[1415] . Although this may seem utopian given the systematic identification of Internet users in compliance with the financial regulations studied, we consider that this new protocol also represents a modest counter-power at the service of cybernauts (which explains the use of the Bitcoin blockchain, which supports these principles of anonymity and incensurability of exchanges). Ultimately, tbDEX is an innovative project, which stands out from the many existing centralized exchange platform projects, notably thanks to the 3.0 IT standards that this service aims to articulate together (P2P, Bitcoin, INAS, DID, VC, ION). Nevertheless, each of these building blocks implies a technical, legal and commercial appreciation and consequences that are as innovative as they are complex to articulate for a large number of society's players. While this new protocol is the first large-scale project to date to combine crypto-assets and IND, it is also a concrete example of an application in the service of a form of universal digital identity, probably utopian as suggested above in the face of political and institutional powers and the multitude of existing legal rules in the financial field.

[1412] "Organizations and individuals (through their portfolios) can be issuers", p.5.
[1413] "In line with the implementation of the tbDEX protocol, the use of analytics and blockchain intelligence solutions can help PFIs to filter, score and monitor portfolios and individual transactions in order to assess transactions against the PFI's risk criteria and regulatory obligations", p.14., *see* also the website of a company specializing in this type of detection www.chainalysis.com or www.ciphertrace.com
[1414] "The protocol has no opinion on anonymity as a characteristic or consequence of transactions", p.1.
[1415] "Our goal is not to maintain transaction anonymity at all costs. Nor is it to undermine an individual's ability to optimize anonymity. In principle, there is nothing to prevent anonymous transactions for financial privacy on the tbDEX network", p.7.

2.4 Identity and the digital euro: cross-analysis of stable crypto-assets and MNBCs

Coins have always been closely linked to the identity and history of human societies. They have been used as a means of communication and social recognition, reflecting the values and beliefs of each culture. The use of money also confers rights and duties on individuals, as John Locke pointed out: "*money plays a very useful part in exchanges, because it enables rights to be preserved in time and space*"[1416] . The term

The word "*fiduciary*" comes from the Latin word "*fiduciarius*", and more precisely from "*fiducia*" ("*trust*")[1417] . Indeed, at its root, money is simply a matter of social trust. In structural terms, fiat currencies such as the Euro, Dollar or Yuan are based on the credibility and ability of one or more States to respect their finances. Today, digital technology has transformed the interactions, uses and societal needs with which money must now contend. For example, in 2021, 71% of adults in developed economies will have a nominative bank account, compared with 42% ten years ago[1418] . Monitoring individuals can potentially lead to the manipulation of their behavior through the collection of information on their habits and preferences, enabling a more or less subtle influence on them. Controlling people's finances can also represent considerable power over their lives, given that capital is a crucial element in many aspects of daily life, such as housing, food, education and leisure. As a result, exercising total control over an individual's finances can have a significant impact on their decisions, choices and general state of mind online today. From this perspective, it is essential to protect the privacy and financial freedom of individuals to guarantee their autonomy and fulfillment. In this respect, the CNIL considers payment data to be "*all personal data used in the delivery of a payment service to a natural person*"[1419] . The arrival of new technological innovations such as crypto-assets has led to a rethinking of the traditional form of money, particularly in its digital form. Over the past 14 years, these innovations have overturned our perception of space and time, as they enable seamless exchanges thanks to decentralized communication between machines, unlike legal tender, which requires the cascading intervention of financial institutions and trusted third parties. While this digital expansion is made possible by the use of our current online currencies, which may lead users to believe that they have a cryptographic underpinning, this is not in fact the case in the sense of the 3.0 technologies we have studied. Today's fiat currencies are nothing more than exchanges of accounting data with legal and economic effects.

[1416] LOCKE John, "Natural law according to John Locke", March 22, 2022, in *Contrepoints.* Retrieved May 22, 2022, from
[1417] Definition of "fiduciary", in *Dictionnaire de français Larousse*, available at larousse.fr
[1418] "The Global Findex Database 2021: financial inclusion, digital payments, and resilience in the age of Covid-19", September 14, 2022, in *World Bank*. Retrieved September 27, 2022, from
[1419] CNIL, Livre blanc n°2 : " Quand la confiance paie ", *op. cit.* available at the following address, p.12.

cryptographically verifiable data carry computer and mathematical effects (crypto-assets).

In reality, the electronic euro is currently not programmable, unlike the cryptographic currencies and their blockchain systems that are the focus of this study. Is it possible, then, for a state or a financial institution to offer a cryptographically and mathematically programmed currency whose exchange rate would be stable and legally recognized? Would a cryptographic euro be legal[1420] ? The recent concept of Central Bank Digital Currencies *(CBDCs) has* emerged in response to certain attempts by private companies such as Facebook to develop stable cryptocurrencies (*see* below). Since the emergence of bitcoin, the volatility of crypto-assets has made these digital tokens an imperfect, but alternative, means of exchange for mass, daily access to goods and services[1421] . While some intermediary solutions exist, such as bank cards enabling crypto-assets to be spent intuitively[1422] , these represent a form of new intermediation that distances these assets and their ecosystems from the initial promises of pure decentralization and minimalist "*zero trust"* social trust previously examined. It appears that these systems, which are more or less computerized and socially decentralized[1423] , but which compete with conventional financial institutions, only imperfectly resolve the problem of the intrinsic volatility of crypto-assets, which depend, as a reminder, on their supply and demand. For the time being, therefore, they are not considered currencies by the international financial system[1424] , with a few exceptions mentioned in the Appendices. For example, central banks are skeptical about the adoption of bitcoin and other crypto-assets, due to their independence and autonomy, their supposed potential for fraud, their economic volatility and, above all, their direct competition with traditional financial institutions.

Faced with these findings, and above all the need for price stability in these unstable tokens, some players in the crypto-asset ecosystem have developed *stable crypto-assets*, known as *stablecoins*. These assets can be linked to the value of another specific asset, such as fiat currency, a commodity or even another crypto-asset (whose price can also fluctuate). Although the concept of stablecoins has been imagined since the early days of the crypto-asset ecosystem, the first stablecoin to date, "Tether" (USDT), was only introduced in 2014 by the company Tether Ltd. The latter is backed by the US Dollar, with which it guarantees parity, so that one USDT is equal to

[1420] De VAUPLANE Hubert, "Is a digital euro legal?", 2023, in *La REF* n°149, Digital currencies and crypto-assets.
[1421] Money only exists through trust, and trust can only be created with a certain degree of monetary stability in the 21st century.
[1422] TELLIER Louis, "Ledger launches its crypto credit card", January 12, 2021, available at agefi.fr
[1423] V. Appendix 7.
[1424] Pursuant to article L.111-1 of the French Monetary and Financial Code, only the euro is legal tender in France. Article 1343-3 of the French Civil Code stipulates that "payment in France of an obligation to pay a sum of money shall be made in euros (...) may be made in another currency if the obligation thus denominated is the result of an international transaction (...)". See also Appendix 5.

a dollar. Since then, other significant stablecoins have emerged, such as the "TrueUSD", introduced in 2018 and also linked to the US Dollar, or the "DAI", introduced in 2017 and backed by a basket of crypto-assets while being linked to the value of the Dollar thanks to algorithmic mechanisms (AEC) mentioned earlier. There are thus several possible and more or less proven methods for guaranteeing the price stability of a *stable digital crypto-asset*[1425] . Since their introduction, stablecoins have gained in popularity as a means of reducing the risk of volatility associated with non-stable crypto-assets (bitcoin, ether). Stablecoins can thus be used for day-to-day transactions (exchange between these stablecoins and crypto-assets), often in ignorance of certain tax rules such as capital gains tax or VAT, which explains why stablecoins are regulated by the MiCA Regulation. Stablecoins have thus found their main use in foreign exchange transactions and the transfer of international funds, also offering a solution for retaining value in countries with unstable economies and/or currencies. However, to fully understand the issues surrounding stablecoins and MNBCs, it's important to consider the differences and similarities that link these two types of crypto-asset. It is possible to run stablecoins on public blockchains, which themselves use a volatile crypto-asset[1426] . This combination can thus lead to challenges in terms of IT understanding as well as regulatory compliance or currency stability.

Since 2014, numerous experimental state and institutional projects for digital currencies in the cryptographic sense have thus seen the light of day (125 projects internationally by the end of 2022)[1427] . Two events have radically accelerated this phenomenon of monetary transition, notably the announcement in June 2019 of Facebook's project to develop a stable crypto-asset (the stablecoin "*Libra*" renamed "*Diem"* before its demise in 2021. Moreover, this announcement effect was accompanied by Paypal's October 2020 announcement that it was now offering the possibility of buying and selling bitcoin and ether to its users[1428] . In the face of this continuing boom in private, stable and volatile cryptocurrencies, traditional monetary institutions have also begun a slow transition towards the development of stable and official cryptocurrencies (SNCMs), i.e., those whose economic and political value would be legally and internationally recognized and

[1425] Three types of stablecoin can be distinguished: (i) fiat-currency-backed stablecoins, which are backed by a pool of fiat currency, such as the US dollar, euro or yen; (ii) tangible-asset-backed stablecoins, i.e. those backed by a pool of underlying assets such as gold, silver or other precious metals, or by commodities such as oil ; (iii) Algorithmic stablecoins, which can be backed by either of the above two types of stablecoin, with the difference that an algorithm is assumed to control its supply and demand to keep its value stable (it is therefore assumed to be highly decentralized and untrusted, unlike the points above); A fourth (iv) type of stablecoin, hybrid stablecoins, combine some of the above characteristics to maximize their stability and security.

[1426] For example, the Ethereum blockchain has its own native crypto-asset with a fluctuating price ("ether"), while at the same time the stablecoin "DAI" offers a stable price and operates thanks to the same blockchain's smart contract. In this way, DAI is linked to ether, but price stability is supposedly guaranteed for the former and not for the latter. DAI is an algorithmic stablecoin, as mentioned on the previous page.

[1427] Consult the interactive map "Central Bank Digital Currency (CBDC) Tracker" by Boston Consulting Group, available at the following address

[1428] V. Appendix 3 & 6, Focus 1 and 2.

cryptographically sound. For example, as early as 2021, China is announcing the official launch of a cryptographic Yuan ("*e-CYN*")[1429] , a profound transformation conceptually initiated as early as 2014 and a priori successful on the monetary and economic front[1430] . Nevertheless, regarding governance and above all data protection for users of this new class of cryptographic asset powered by central banks, abuses seem possible (targeted, mass surveillance, censorship). On October 2, 2020, the ECB published a report on the Digital Euro[1431] , whose vocation would be monetary and whose underlying cryptographic (potentially incorporating certain blockchain standards). The provision of a cryptographic Euro for European citizens represents something of a reaction by the ECB to the aforementioned stable and volatile crypto-assets and e-CYN. According to a decision by Christine Lagarde, President of the ECB, the idea of officially launching a crypto Euro was taken on October 23, 2023[1432] , for implementation in 2026 or 2027, according to the Banque de France[1433] . This would be an interbank cryptographic Euro[1434] also accessible to the general public[1435] . It could be centralized or decentralized in IT terms, but would probably be centralized or hybrid in the sense of this study. Indeed, a centralized system would enable IT control and infrastructure centralization to be maintained, in line with state governance mechanisms and the multiple legal rules associated with today's currencies. Comments by the Governor of the Banque de France in 2022 suggested that central bankers are looking for ways to integrate tokenization functionality into the existing monetary architecture (particularly useful for closed blockchains)[1436] , while regulating the technology appropriately[1437] . The crypto Euro would therefore probably be a public, digital currency that would operate in a similar way to cash, i.e. available on a peer-to-peer basis for retail payments (thus creating a legally recognized "electronic cash 3.0")[1438] .

[1429] "Progress of Research Research & Development of E-CNY in China". 2021. pbc.gov.cn

[1430] GAYTE Aurore, "261 million people used the app to pay with e-CNY"*;* "Tout comprendre au e-yuan, la monnaie numérique que la Chine met en avant pendant les JO 2022. Plus de rapidité mais moins de vie privée?", February 4, 2022, in *Numerama.com*, available at Numerama reading, see also SLIM Assen, "La MNBC e-hryvnia: une monnaie banque centrale en projet", November 29, 2022, in *La REF*, n°147, "Les monnaies numériques et les crypto-actifs". [1431] ECB, "Report on a digital euro", 2020, available at ecb.europa.eu

[1432] BARLUET, Alain, "Les étonnants canulars d'un duo russe au service du Kremlin", 2023, in *Le Figaro*, available at

[1433] VILLEROY de GALHAU François (speech) "Anchors and catalysts: the dual role of central banks in innovation", "In Europe, we are halfway through our study phase: the Eurosystem will make its decision by the end of 2023, for a potential launch in 2026 or 2027", Banque de France. Available at

[1434] *Ibid*. Reference is made to the "Wholesale Digital Euro", i.e. an implementation of a digital euro only accessible and usable between financial institutions (between commercial banks and/or with the ECB).

[1435] *Ibid*. Reference is made to the "*Retail Digital Euro*", i.e. the implementation of a digital euro accessible to all without distinction, European citizens, financial institutions and retailers.

[1436] The advent of a *cryptographic euro* will make it possible to finance the infrastructures of private and hybrid blockchains, ecosystems in need of financing as previously mentioned by this study. See below.

[1437] VILLEROY de GALHAU François (speech), *op. cit.* "I hope that we central bankers will find a way to integrate tokenization into the existing [monetary] architecture, while regulating it to the extent necessary," available at.

[1438] It should be pointed out that this very term was mentioned in Bitcoin's White Paper as early as 2008, which shows that the ECB's intention is in line with Bitcoin's desire to create an *electronic cash*, with the difference that a euro

The ECB's political objective seems to be to maintain the role of currency 2.0, in the 3.0 era, by offering a transition supposedly at the service of European citizens and their economic and financial rights (right to an account, administrative simplification, etc.). The adoption of a cryptographic Euro would also theoretically preserve the role of the EU's official currency as a stabilizer of the payment system, while transposing online the use of cash that persists while gradually declining[1439] . A Euro 3.0 would supposedly help protect this monetary sovereignty while promoting competition in the provision of new banking and financial services. In addition, the cryptographic Euro could accelerate the digitization of the European economy. Where there is competition between a private currency and a public, official currency managed by a central bank, the latter has a duty to provide certain responses, particularly in terms of standards and policies, to the phenomenon of crypto-assets, whose monetary vocation was originally private, then finally opened up to the general public[1440] . The MiCA Regulation proposes some initial responses, notably by imposing direct supervision of "*significant*" stablecoins[1441] (in terms of volume and origin) by the European Banking Authority *(EBA*). With a cryptographic Euro or Dollar, central banks aim to inspire confidence in society once again, by providing a new 3.0 medium of exchange directly and cryptographically linked between citizens and central banks. One of the ECB's main challenges is therefore to transpose the existing trust in financial institutions to the supposedly more inclusive and secure 3.0 digital trust of such a cryptographic Euro. This transition is not trivial, as it must be accompanied by social, IT and legal justifications and foundations commensurate with the supposed impacts. For example, it will be necessary to carry out contextualized identification for users[1442] , whether they are natural persons (European citizens) or legal entities (financial institutions, merchants). This prior identification would make it possible, in particular, to prevent the "*Sybil attacks*" mentioned[1443] , while also enabling legal action to be taken in the event of fraud or illicit activity. The ECB should therefore put in place solid identification and IT security mechanisms to guarantee user confidence in this Euro 3.0. For a cryptographic Euro to become a mainstream solution

---

will be legally regulated and recognized. V. *op.cit.,* NAKAMOTO Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008, available online.

[1439] NEDELEC Gabriel, "Le cash continue son lent déclin en Europe", in *Les Echos*, 2020, "Les paiements en espèces ont représenté 73 % de l'ensemble des transactions réalisées en 2019 dans la zone euro", available online. Often evoked, the disappearance of cash would probably mean de-banking for people in irregular situations, which does not seem desirable for these most modest players in society.

[1440] ROCCA Olivier, ACHER Vincent, DENIS Philippe, SALLET Fleury, "In defense of banks and states, we can affirm that before the arrival of the Bitcoin public blockchain network, the notion of public [cryptographic] currency did not exist", Protocole Executif, 2022, in *DUDM*, available at the following address, p.43.

[1441] See *supra,* I, Title 2, 2.5.1.

[1442] ECB, "Report on a digital euro", *op. cit.* p.38, "The issuance of a digital euro should remain under the control of the Eurosystem. Supervised intermediaries should be involved at least for the identification and on-boarding of authorized users and possibly for the routing of transactions to the central bank's infrastructure; they could create new businesses on digital services related to the euro", ecb.europa.eu

[1443] *Ibid.* p.28.

As a global, reliable and sustainable service, it is essential to make it technically affordable and accessible without constraints, with or without Internet, via mobile or computer, with the programmed possibility of pseudo-anonymity for transactions. The aim of these features is to improve financial inclusion, particularly for non-European individuals present on European soil, whose banking status is currently precarious or non-existent. One likely solution is to make this cryptographic Euro available to European citizens via a distributed digital identity (PIND). Such an interweaving of 3.0 digital identities and a means of payment

3.0 implies secure, sovereign, simple and rapid management and use of cryptographic identity and payment data. The identity verification processes (KYC)[1444] of users of these digital wallets would thus require the harvesting and sharing of root identity attributes for their users and by the financial institutions concerned. In any case, thanks to an IND, verification of bank identity information would be simplified, as it would be automated, thus avoiding scams and difficulties relating to liability and violations of the rights of the users or institutions involved[1445] . To illustrate this point, in November 2022[1446] , the Banque de France closed a call for contributions on the subject from the BPCE group and the companies Archipels and IN Groupe. The use of an IND in the management of authentication for credit institutions is officially mentioned, which seems to confirm this possibility.

In the light of these remarks, it seems pertinent to compare the positioning of bitcoin since 2009[1447] , to the initiative of the cryptographic Euro, which draws certain cryptographic and technological inspirations from its blockchain (almost 20 years on). For the first time, the emergence of bitcoin has enabled private and digital players to invest themselves with monetary power, in the sense of the three functions of a currency as defined by Aristotle[1448] . This situation is unprecedented in the digital age, and it is difficult to foresee the implications of such a reversal of hitherto established financial powers. As a whole, economists, politicians[1449] and many

[1444] The sharing of Verifiable Attestations (VAs) between banks could be done in the short term and in a simplified way, as banks already trust each other electronically and socially in their financial ecosystem. This would be an improvement (using VCs) over using and sharing KYC (PDF, photos, Web 2.0). [1445] OTTAWAY Catherine, "Les banques sont responsables en cas d'ordre de virement électronique irrégulier", 2002, in *Les Echos*, accessed October 13, 2022, available at the following address, see also Cass. com. November 2, 2016 n° 15-12.325 and Cass. Com. January 24, 2018, n° 16-22.336
[1446] Banque de France, "The Banque de France closes its call for contributions on the use of digital identity in the banking sector. authentication management for credit institutions", "A collaboration of IN Groupe (Imprimerie nationale) and Orange, to implement decentralized identity on Blockchain technology", 2022, available at [1447] NAKAMOTO Satoshi, free translation from English, "Many people automatically consider e-money a lost cause because of all the failed ventures since the 1990s [B-Money, DigiCash, Hashcash already mentioned]. I hope it's obvious that it's only the centralized nature of these systems that has doomed them. I think this is the first time we've tried a decentralized, non-trust-based system", 2009, available online at
[1448] V. Appendix 3, Focus 3.
[1449] DUFRENE Nicolas, DELAHAYE Jean-Paul, MAUREL Emmanuel, et al, "Les crypto-actifs : du mirage à la réalité penser l'impact financier, économique, écologique et politique des crypto-actifs", "For the time being, however, we're struggling to find really decisive arguments that would demonstrate the social added value brought by cryptoactives. On the contrary, it has to be said that the cryptoasset ecosystem provides at best a facsimile of the traditional financial and banking system, without having the same assets, starting with the legal ability to create money, and above all

governments have regularly questioned the computing, monetary and financial potential of this asset, ever since it first appeared on the scene and as it has been adopted by Internet users. Central banks and institutional and political circles are mainly opposed to Bitcoin for at least three reasons. Firstly, Bitcoin is beyond the control of central banks and governments, calling into question their role as guardians of monetary policy and financial stability. This loss of control represents a threat to their monetary sovereignty and economic profitability, as Bitcoin enables valuable tokens to be transferred and stored without intermediaries. Central banks also consider Bitcoin to be a vector for fraud, money laundering and the financing of illegal activities, despite reliable figures to the contrary[1450] . Finally, the powers that be believe that the high volatility of Bitcoin's price is a major concern, as it can disrupt the functioning of the economy and create instability on financial markets, a postulate that today seems complex to demonstrate scientifically. In short, central banks and political and institutional circles perceive this infrastructure and token as a threat to their traditional role, monetary sovereignty and international financial stability. In reality, it's important to understand that most of these concerns are based on sometimes preconceived ideas, and that Bitcoin can also offer advantages to all Internet users as a fast, inexpensive and secure means of payment. Based on this observation, which is examined in the Appendices[1451] , the fundamental question to be answered is: what exactly would an MNBC offer that bitcoin or stablecoins do not? Before offering some thoughts on this fundamental question, some of Satoshi Nakamoto's words, written in 2009, help us to understand the origin of this monetary competition between accounting versus cryptographic and mathematical digital currencies:

"We have to trust the central bank not to devalue the currency, but the history of fiat currencies is full of violations of this trust. (...) *We need to trust them to protect our privacy, so they don't let identity thieves drain our accounts*"[1452] . So, would the launch of MNBC really enable central banks to generate a new level of trust among the citizens for whom this new form of 3.0 exchange is intended? In 2021, the CNIL reminds us that respect for privacy and protection of personal data are essential to guarantee a trusted currency[1453] . The ECB explains that the cryptographic Euro would simply be a digital extension of fiat money, and in particular of cash, such as

---

without any of the safeguards that have gradually (and still incompletely) led to a framework for the actions of banking and financial players", 2022, available at the following address, p.105.

[1450] Worldcoin, "Understanding Money Laundering: How Common Is It in Crypto?", 2023, available at, "In a separate report by CipherTrace, the total volume of illicit crypto-currency transactions was between 0.1% and 0.15% in 2021. This figure was closer to 0.62-0.65% in 2020. Cash remains the most common medium of exchange used in money laundering".

[1451] V. Appendices 3 & 6

[1452] NAKAMOTO Satoshi, "Bitcoin open source implementation of P2P currency", 2009. P2P Foundation. Accessed at

[1453] CNIL "Livre Blanc n°2 : Quand la confiance paie", *op. cit.* available at the following address

mentioned above. The essential feature of transaction anonymity would therefore have to be guaranteed by law[1454] and then by IT (e.g. VC, DID, ZKP). Similarly, data protection would be protected to varying degrees depending on the technical choices made, so as to arbitrate between individual rights and the technical efficiency of this centralized but legally recognized MNBC. Whereas the regulation of fiat currencies allows complete anonymity for cash exchanges, the regulation of electronic payments with an MNBC[1455] would probably only allow pseudo-anonymity at best[1456] , in line with the many European texts on AML/CFT that have been mentioned (MiCA, TFR). Thus, reliable identity verification processes will be required under the relevant regulations[1457] , depending on the amounts, transaction frequencies and profiles of each individual. In theory, their identity and transaction history will only be visible to the central and/or commercial banks that the user has deliberately chosen. In reality, however, this cryptographic Euro will have to address the issue of state "censorship" of citizens' private financial transactions. Indeed, the introduction of an MNBC could make it possible to censor or massively monitor certain citizens, at any time, in real time[1458] and according to a legal framework in perpetual mutation as demonstrated. Today, this does not apply thanks to the alternative of cash, which represents a protective halo of anonymity for citizens in the face of all unjustified attempts at widespread control and surveillance (which bitcoin also originally represented). In 2021, the French Data Protection Authority (CNIL) is highlighting the risks of over-identification linked to the purposes and uses of a cryptographic Euro or, more broadly, any MNBC[1459] . The risk of data leaks is just as likely, and as happens regularly in the world of crypto-assets (responsibility often lies with users and online services, and not with states as might be the case with an MNBC). Furthermore, from an economic point of view, the introduction of a programmable crypto Euro offers the possibility of setting up a 'melting currency'. Such a currency could include an expiration date, obliging citizens to use their funds before a certain period, failing which the cash would become unusable. This feature could,

[1454] In accordance with the protection of the right to privacy and the right to protection of personal data, as well as freedom of expression and secrecy of correspondence.
[1455] ECB, "Report on digital euro", *op. cit.* Requirement n°10, p.20, available on ecb.europa.eu
[1456] In other words, unlike an MDBC, cash is almost impossible to censor once it has been physically distributed to citizens, as peer-to-peer exchanges are mostly anonymous and untraceable.
[1457] *Know Your Customer (*KYC) process enabling systematic identification of users of financial services, in accordance with Directives: Directive 2009/110/EC of September 16, 2009 (in force); Directive 2015/849/EC of May 20, 2015 (in force); Directive 2013/36/EC of June 26, 2013 (in force); Directive 2018/1673/EC of October 23, 2018 (in force); Directive 2018/843/EC of May 30, 2018 (in force); Directive 2019/1153/EC of June 20, 2019 (in force).
[1458] STACHTCHENKO Alexandre, BALVA Claire, "Bitcoin & Cryptomonnaies Faciles - Comprendre Les Monnaies Numériques Et Leurs Enjeux Économiques", Éd. First, 2022.
[1459] CNIL, "Livre Blanc n°2", *op. cit.* p.21, "In addition, reflecting the polysemy of the term 'identity', there are several levels of identification, ranging from the anonymity of cash use to the government-certified identity, via the declarative identity or pseudonym via a login and password. In most contractual payment transactions, the use of a declarative identifier from the merchant or the subscribed service is sufficient, and a 'regalian over-identification' for authentication purposes would not be desirable".

certainly be beneficial for States, which could thus encourage consumption or savings, but this introduces the risk of these mechanisms being used for purposes that are more or less pragmatic from a conceptual point of view.

It's worth emphasizing that when people are unable to carry out private financial transactions, they lose part of their rights. Financial freedom or access to a reliable currency is intimately linked to many other rights (to work, to travel, to healthcare). While these rights and freedoms are generally enjoyed in developed countries with reliable currencies, the situation is much less clear-cut in many developing countries. For the latter, for example, the high transfer fees imposed by financial intermediaries are an insurmountable obstacle for many populations, who are therefore looking for alternatives. Stable crypto-assets can help reduce these costs considerably, and ultimately improve the financial situation and lives of these individuals. This is a particularly useful solution for citizens in developing countries, who are hardest hit by the high costs of transferring funds. Today, the most proven and reliable cryptographic asset on the Internet is bitcoin. Its computing capabilities, which have been studied in the Annexes (Lightning Network, Taro)[1460] , its political independence and its global resilience make it a useful monetary asset for exchanging goods or services in complete confidence via the Internet. Yet its volatility remains an obstacle to its global adoption as a currency. It thus seems that it cannot replace the traditional financial system, but rather helps to reinvent it, as demonstrated by the many MNBC launch projects around the world. The traditional payments system is fragmented by nature, with a whole ecosystem of players to authorize, carry out and then record payments, whereas the Bitcoin blockchain conceptually unites all this on a single, public, digital ledger. In practice, Bitcoin would not be able to support all the annual transactions carried out by today's payment systems in the short term. In the medium and long term, however, there are a number of possibilities for meeting such needs, subject to social and political acceptance, including on the energy front, which is also explored in Appendix 6[1461] . More generally, since around 2013, political announcements against the crypto-asset sector - stable or unstable - seem to be multiplying, rightly and wrongly. Wrongly, concerning the computing and economic capabilities and applications of the Bitcoin and Ethereum protocols[1462] , but rightly concerning their legal inadequacy and uncertain monetary adoption for the time being. By way of illustration, the Bank for International Settlements (BIS), which is responsible for

[1460] V. Appendix 3, Focus 4.
[1461] V, Appendix 6, Focus 1.
[1462] As of 2018, the Banque de France considers that "bitcoin is neither more nor less than a speculative object", DUPUY Caroline, "Cryptomonnaies: how does it work?", 2018, in *Les Nouvelles Publications*, available at, *v.* also.
"Crypto-economic warfare, MNBC, stablecoins: What is the Banque de France doing?" Cryptoast, 2022 [Video]. YouTube.

promoting international monetary and financial cooperation with regard to CBMs[1463] , considers in a June 2022 bulletin that "*blockchains* (...) *present negative network externalities. The more transactions a given user carries out on a blockchain, the more it clogs up the system, and the higher the transaction costs for everyone else. Even if everyone wanted to transact in the same crypto-currency, congestion would lead to the proliferation of new currencies*"[1464] . In its annual report of the same year[1465] , a comparative table demonstrates the supposed superiority of the BIS vision for the monetary system of the future. In fact, eight key criteria for any monetary system are cited[1466] to compare chronologically (i) the current monetary system, (ii) the crypto-asset alternative and (iii) the BIS vision of the optimal monetary system for the future (MNBC). According to this table and the BIS data, the results are clear: the traditional monetary system currently meets only one out of eight criteria, while crypto-assets meet two out of eight, and MNBC systems supposedly meet eight out of eight. It would seem, therefore, that these results can be put into perspective due to the ongoing innovation of the crypto-asset sector and the multiple parameters and findings evoked by this thesis. As a result, this report's finding of a promising future for CBDMs is based on a relatively biased premise, as institutionally motivated by the desire to preserve the current financial order and its oligopolistic operation. The objective of CBDMs is to compete with crypto-assets so that the traditional financial system does not risk seeing its current predominant role largely redefined. To prevent this from happening, policies and regulations are being put in place, under the guise of sometimes questionable justifications[1467] and oriented in favor of MNBC currencies, which are dispensable at present. Once again, it seems that the banking world's views on crypto-assets are subjective and political, and not objective and educational enough at present. It is suggested in this study that if the value of a currency rests on its massive use, then bitcoin is an admittedly imperfect currency, but undoubtedly one in the making. The use of bitcoins by a growing group of users confers on it an almost certain social and economic value, of which there is no doubt.

[1463] CNNum, "Anonymity and universality: key issues in the development of digital currencies", interview with Eric Monnet (Director of Studies at EHESS), "The United States and Europe are at the same point on these issues. They support both a desire to accelerate regulation, particularly around bitcoin, and to issue a central bank currency. This position is shared by all the central banks of the industrialized countries, which are grouped around the Bank for International Settlements", available at the following address

[1464] BOISSAY Frederic, CORNELLI Giulio, DOERR Sebastian, FROST Jon, "Blockchain scalability and the fragmentation of crypto", BIS Bulletin n°56, June 7, 2022, available online at, p.7.

[1465] BIS, "Annual Economic Report 2022", p.77, available at

[1466] *Ibid.* "security and stability, accountability, efficiency, inclusion, user control of data, integrity, adaptability, openness".

[1467] For example, new rules in EU law aim to directly limit payments in crypto-assets via the introduction of a ceiling of 1,000 euros below which anonymity remains, and above which identification will be systematic and mandatory. Such rules thus curb the monetary adoption potential of bitcoin, which was not designed to adapt to a particularly strict legal framework. v. article by Jean-Luc, "Le Parlement européen souhaite plafonner les paiements en actifs numériques", "To restrict cash and crypto-asset transactions, MEPs want to cap the payments that can be accepted by people providing goods or services. They set limits of up to 7,000 euros for cash payments and 1,000 euros for crypto-asset transfers for which the customer cannot be identified.", 2023, available on bitcoin.fr

monetary recognition would be an increasing function of its adoption[1468] . It should be noted that bitcoin is already legal tender in two jurisdictions (El Salvador[1469] and the Central African Republic[1470]), where goods and services can be traded. Although the democratic legitimacy of these countries may be called into question by Western powers, the use of bitcoin enables these countries to open up to the world of information technology, ultimately representing a source of economic and social growth for them. Computationally and socially plausible, but politically utopian given the current state of banking and government powers, bitcoin could replace MNBC as a means of reintroducing scarcity into society's economic and digital system. It should be noted that a cryptographic euro's primary vocation would be as a means of payment, and not as a means of investment, as is often the case. Based on this premise, a euro 3.0 would compete with bitcoin only in the payment segment, and not in the investment segment, which is not part of its purpose. It therefore seems both possible and desirable to stop pitting Bitcoin against MNBCs, in favor of their complementarity and future coexistence. Bitcoin's computational resilience and intrinsic cryptographic scarcity make it a monetary counter-power that liberates people financially and partially socially, provided that the players in today's financial and economic system allow it to do so to some extent. In the pre-launch phase, it still seems early to assert the legal and social soundness of the massive deployment of a cryptographic euro and its future links with crypto-assets. The stable crypto-assets already in circulation and accessible within the EU will be the subject of particular attention and scrutiny by the European legislator, given their particularly competitive positioning. Finally, it seems imperative to guarantee strict protection of anonymity during the likely rollout of a cryptographic euro, to ensure the online continuity of the physical model of a hard currency that has already proved its worth in terms of social consensus. In view of bitcoin's gradual adoption, only its social adoption could enable it to become a cryptographic and perhaps monetary commons, i.e. a universal cryptocurrency, despite its unstable price and minority legal recognition to date internationally.

[1468] V. Appendix 3, Focus 1, 2, 3 and 6.
[1469] V. Appendix 5.
[1470] Les Echos, "Le bitcoin devient une monnaie officielle en Centrafrique", 2022, available at

Conclusion of the second part

The second part of this study introduces and explores the concepts, functioning and potential of third-generation digital identity standards, which will play a decisive role in the Internet's 3.0 future. The hypothesis of a legal and digital identity strengthened by the transparency and openness of these new cryptographic standards is confirmed, on condition that it is accompanied by a form of digital identity intermediation, not totally decentralized, but rather distributed on an IT and social level. A legal analysis of the eIDAS Regulation and its proposed amendment (eIDAS-2) highlights the coherence between guaranteeing the online and offline legal identities of European citizens. With the advent of converging technologies and the legal rules that will soon apply to them, a number of structural and complementary recommendations are suggested for framing and safeguarding 3.0 technologies, whether their vocation is financial or identity-related. A practical analysis of some highly decentralized projects shows that, while it is now possible to achieve a universal digital identity, this concept remains utopian for the time being, due to the diversity of legal and political systems, sometimes with little or no harmonization in the countries concerned by this notion. It is therefore possible to issue decentralized proofs of existence on public blockchains, but for them to be legally recognized by one or more legal systems, it is essential for public authorities to be involved in the process of issuing digital identities. In this way, the issuing and recognition of digital identities becomes distributed rather than decentralized, once an entity is legally recognized. In France and the European Union, political and legislative bodies are gradually having to distinguish between the notions of IT decentralization, which concerns digital identity, and that which concerns crypto-assets. For the time being, these two use cases are distinct, yet widely confused by these institutions and consequently by the general public. This reinforces the fact that the time for regulation must not be reduced to that of innovation, which is often faster and more immature, as demonstrated by the majority of 3.0 solutions, too often supposed to be decentralized and reliable. It is also important not to banish the most open and decentralized infrastructures and technologies, as a minimum degree of decentralization should always be possible and accessible to Internet users in need of or seeking emancipation and/or digital freedom(ies).

Conclusion

The scope of the notion of identity is so vast that it must be circumscribed in order to be analyzed in terms of philosophy, the social sciences and the rules of law. Through observation of a number of historical forms of expression of personal identity, it has been shown that identity has always been socially organized and centralized within hierarchically structured social systems and institutions. Each human being produces his or her identity at the same time as he or she produces the collective identity of his or her fellow human beings, according to one or more cursors specific to each culture and society. Today, as the need for identity grows with the world's population, the boundaries of identity are expanding in the digital age. While many 2.0 and now 3.0 digital solutions exist, millions of people still struggle to prove their identity and are denied this fundamental right. This study has suggested that identity needs to be understood in terms of the contexts in which it is used, either individually, collectively or both, depending on the use case. The concept of a global identity is introduced, with reference both to the subjective feelings of identity that each person may experience, and to their legal identity established by civil status. These notions are as essential as they are complex to define, as they fluctuate according to socio-cultural environments. Three interdependent components of any identity have therefore been chosen as the focus of study: biological identity, legal identity and psychosocial identity. For simplicity's sake, these components have been grouped into two categories, the first designating primary identity attributes (biological and legal identity) and the second designating secondary identity attributes (psychosocial identity).

It has been shown that trust and intermediation are intimately linked and play a crucial role in Web 2.0, with each Internet user having to trust multiple identity and online service providers to enable them to express their digital identity and interact with those of other users. Our study of the technological context and legal framework for digital identity in Europe has revealed a number of limitations specific to 2.0 digital identity. The need to redefine Web 2.0, i.e. to reinforce online identity with certain new Web 3.0 technologies, appears to be a necessity for Internet users. Indeed, blockchain technologies and decentralized digital identity (IND) give new meaning to and reinforce the founding notion of digital trust, thanks to new, more secure data transmission mechanisms. These new technologies are shaping an unprecedented new computing environment for expressing and asserting citizens' rights online, notably in support of unprecedented financial freedom and programmed data confidentiality. The growing number of Internet users holding crypto-assets, for example, are likely to hold verifiable cryptographic credentials, i.e. to adopt a distributed primary identity and a - financially - decentralized secondary identity. This study highlights the need to liberate identity

and social identity, while reinforcing the exercise of their rights when surfing online. Given the current state of technologies and their applications, it is becoming urgent for cybernauts to move from a passive to an active digital identity. To achieve this, we encourage every citizen to carry out a digital identity check, as suggested by French academician Amin Maalouf in 1998, with regard to our global and psychosocial identity.

This study proposes a balanced approach to the next type of digital society, with its distributed and decentralized IT resources. It introduces and encourages a pragmatic and up-to-date legal and IT perspective on these new 3.0 technologies and their applications, far from preconceived ideas. The study also demonstrates that IT decentralization is not appropriate in all cases. Nevertheless, a high degree of IT decentralization remains essential for the trust placed in cryptocurrencies, digital shields and certain fundamental rights, for example. This phenomenon of IT decentralization can only be achieved by a handful of computer networks, as is the case today with the Bitcoin blockchain. What seems most opportune is to seek to decentralize, and ultimately disintermediate, certain areas of activity such as digital identity. In 2023, there remains an inseparable link between the IT concepts of blockchains and those of crypto-assets, an observation that also applies to private and hybrid blockchains, which will probably be tokenized in the future thanks to the digital currencies of central banks, whose mechanisms will be legally recognized and technologically centralized by the public authorities. Thus, the opposition between open versus closed 3.0 technological bricks is likely to intensify in view of the texts and legal rules currently being adopted, and partly fueled by a political will to control and frame these social phenomena of digital decentralization initially conceived for the people and in the service of their online emancipation.

The growing adoption of crypto-assets by businesses, individuals and a few (quasi)states demonstrates the socio-economic emulation brought about by certain distributed applications (fund-raising in crypto-assets, issuance of stable tokens, decentralized companies). However, the ease with which an Internet user can create a token or a decentralized digital application is often perceived by legislators as a risk for investors and citizens. This is why the first founding texts for the future of these 3.0 technologies are emerging in Europe. This is currently the case for decentralized identity and crypto-assets, with the aim of providing a framework for these ecosystems and their players, to the point of directly or indirectly constraining the ecosystems of the most decentralized infrastructures. For players in the crypto-asset ecosystem with a low or medium degree of decentralization, regulatory compliance will be their top priority over the next few years (MiCA, TFR), as their overall survival depends on it. This observation is also shared for decentralized digital identity (RGPD, eIDAS-2, Data Act), especially when primary identity attributes will be involved to identify natural persons. This research introduces

a new way of looking at blockchain technologies in terms of digital identity and finance 3.0, allowing them to coexist with varying degrees of decentralization, from the most legally compliant (closed blockchains) to the most ambitious and sometimes non-compliant (open blockchains). It seems futile to attempt to control all these constantly evolving technological expressions, especially those whose protocols are designed with a high degree of resilience and IT decentralization in mind. Some countries, such as France, are gradually adopting a legal framework that, while providing legal certainty and attracting new foreign players, also generates numerous constraints for the players in these Web 3.0 ecosystems. The risk is that these French players will become less competitive, to the benefit of foreign players who are financially and commercially stronger due to more flexible and less restrictive legal systems. In theory, the challenge of this recent strengthening and tightening of the regulatory framework applicable to crypto-assets[1471] is to ensure effective and equitable application to all players in this ecosystem, including foreign players who address the French market without legal registration (PSAN), as analyzed in this study.

Ultimately, a balance needs to be struck so that crypto-assets do not form a world apart from society, but rather one of its new future dimensions. It is desirable to think of the law in terms of the use cases of blockchain technologies, i.e. with legal rules and cryptographic tools adapted to the concept of decentralization. A single, global regulation applicable to blockchain technologies has been ruled out, as there are in fact multiple variants for each 3.0 technology, as many as there are sometimes contradictory legal rules. As a result, it is not the technologies used by blockchains that need to be regulated, but rather their uses. The links between the concept of personal responsibility and cryptography advocated by Web 3.0 ("*lex cryptographia"*), and the intervention of a third party, make it difficult for Internet users to understand. Indeed, the more decentralized a solution is, the less intuitive it is for its users, and those least digitally literate will prefer to trust a competent third party by delegating cryptographic responsibility for their crypto-assets and/or identity attributes. Digital trust thus always implies social trust, and it is up to the legislator to balance the articulation between these two possible perceptions, both in terms of responsibility, and on a case-by-case basis depending on the level of decentralization of the 3.0 solution.

This study concluded with a computational and conceptual distinction between the notion of decentralized digital identity (IND) and that of self-sovereign digital identity (INAS). Understanding decentralized digital identity means overturning our current perception of digital identity. The user is evolving from a relatively static identity, locked in and dependent on an online service, to a new, dynamic one, in which he or she becomes the cryptographic owner of his or her own digital identity.

[1471] ADAN, "Enregistrement renforcé des PSAN : quel bilan après le vote du projet de loi DDADUE ?", 2023, in *adan.eu*, available online

of each and every one of its digital data and traces. This shift from a centralized 1.0 and 2.0 IT identity to a decentralized 3.0 identity opens up new perspectives for every online relationship and interaction. It facilitates access and communication both online and offline, while reducing the risk of identity theft and data breaches. The use of pseudo-anonymous cryptographic identifiers, partially proprietary and minimized by design under the RGPD, gives users of this new technological concept serious advantages over existing ones. Coupled with legally recognized blockchain technology, IND increases and ensures the transparency and quality of exchanged data. Currently undergoing legal, political and industrial recognition at EU level (eIDAS-2), IND will represent an essential new cryptographic protection foundation for European citizens within the next few years. However, France is lagging behind other European countries, such as Germany and Spain, in the development of this new technology, which lacks political recognition and support. For the time being, it will still be some time before the idea of digital trust 3.0 is accepted by the general consciousness to the point of unanimity. Distributed or decentralized computing attracts as much as it dazzles. Until it is adopted, it creates a form of resistance for those accustomed to centralized trust systems, who find it hard to break away from them. The high degree of decentralization attached to the concept of a self-sovereign digital identity introduces the concept of a universal digital identity. Coupled with a public blockchain, the INAS concept could for the first time enable the birth of a universally accessible and open digital identity. In other words, the use of IND or INAS would provide a universal proof of existence for every human being, enabling them to access rights that are also decentralized, such as a universal income in crypto-assets, for example. This cryptographic proof of existence must, however, be linked to fundamental rights, which only a constitutional state can guarantee.

So, while achieving a universal digital identity is desirable thanks to a public blockchain that would host unforgeable digital proofs of existence, this possibility seems utopian for the time being due to the lack of maturity and recognition of Web 3.0. Consequently, only a proof of existence attached to a distributed, semi-centralized digital identity can provide a legally recognized link with a trusted third-party identity provider and de facto legal recognition. This study favors the use of distributed identities, i.e. computer hybrids rather than completely decentralized ones. Today, the majority of online identification situations require civil identity attributes, necessarily originating from a trusted third party, often public and state-owned. Without the advent of decentralized metavers or self-proclaimed quasi-states, the lex cryptographia dear to Web 3.0 cannot stand alone, as it cannot cover and guarantee all the complexity of social relations. However, it undoubtedly helps to improve them by offering new digital alternatives and perspectives, particularly for the online identity attributes of Internet users.

The market for decentralized or distributed electronic registers is currently driven by open blockchains, which are favored by small, innovative companies for economic (need for financing), commercial (search for a network effect), IT (resilience) or, more marginally, regulatory (search for the least restrictive jurisdictions) reasons. At present, the focus is shifting from a Western perception of public blockchains to a more pragmatic perception of their importance and necessity in developing countries. Consequently, forcing public blockchains in the West through law is tantamount to preventing their legal and social adoption in developing countries, where they are most needed. In these countries, where states can be unstable or corrupt, a public blockchain represents an open and trusted electronic register, whose identity and monetary functionalities offer new methods of governance. Public blockchains therefore represent a form of counter-power and a universal digital commons, from which developed countries can also benefit in the event of a deterioration or retreat of democracy.

However, it is also necessary to recognize that not all public blockchains are capable of responding to some of society's challenges, particularly with regard to primary and regal digital identity, which for the time being requires the use of private or hybrid blockchains. As a result, no decentralized infrastructure can claim to meet all needs and use cases, as is often promised by certain Web 3.0 players. Conversely, no private or hybrid blockchain can claim to be, or call itself, a decentralized infrastructure, but a distributed one at best. A balanced and contextualized perception of each technology is therefore necessary to qualify the legal stakes of these contexts and their financial and/or identity 3.0 solutions as closely as possible to reality. We have also observed that the more functional a blockchain technology is, i.e., the greater the number of use cases it hosts, the greater its surface area and the greater its likelihood of cyber-attack. While no public blockchain is immune to a flaw or breach, their community and governance make them considerably less so than private and hybrid blockchains. At the same time, the more a decentralized solution is adopted by a large number of users worldwide, the more likely it is to be strictly regulated by the legislator. Finally, all the regulatory approaches discussed in this study are partial and imperfect solutions, given the constant evolution of these new technologies. The point is not to prohibit, but rather to preserve certain primitives of blockchain technology in order to observe whether new social and digital models can emerge, as was the case with the Bitcoin protocol.

This research suggests that this protocol represents a Copernican revolution, as its creation radically transforms the current monetary and financial system, just as Copernicus' discovery overturned the understanding of the universe in the 16th century to the point of impacting every future generation. It has been demonstrated in the Annexes that Bitcoin tends to be more of an infrastructure than a system.

service of a universal common good, than a pirate infrastructure designed for illicit purposes, as is often portrayed by the media and then understood by the general public. The monetary, financial and probably identity revolution exemplified by the Bitcoin infrastructure should neither be favoured nor forbidden[1472] , but rather tolerated and studied with great attention by the public and private players in society. An examination of a number of ground-breaking projects by major technology companies such as Microsoft (ION project), Twitter (tbDEX project) and certain IT upgrades (Lightning Network, Ordinals) suggests that the potential and adoption of Bitcoin infrastructure is still in its infancy. A study of the history of technology shows that what seemed unimaginable yesterday, such as the recognition of Bitcoin as a legal tender in El Salvador, could well be unavoidable tomorrow. This research suggests that public blockchains should no longer be underestimated or discriminated against. For now, the Web

Web 3.0 is mainly based on these open infrastructures, of which only the Bitcoin blockchain is actually stable, reliable, transparent and proven, and likely to endure, unlike the many other decentralized applications and promises of Web 3.0. The time has come to initiate a pragmatic democratic debate on the contributions and challenges - IT, economic and social - that Bitcoin brings to our ultra-digitalized, yet fragile, society. In the meantime, the best weapons for Bitcoin to win its place in society by fighting political and institutional attacks are to inform and educate Internet users. To find out whether Internet users and citizens will prefer a decentralized IT infrastructure that is resilient, but not very legally compliant and monofunctional, or a centralized infrastructure with multiple functionalities that is legally compliant, but not very resilient, our study suggests that Internet users will prefer a blockchain that is resilient for currency 3.0 (Bitcoin) and less resilient for their digital identity.

3.0 (closed blockchains), each responding to different needs and uses. While Internet users have a natural need to trust a third party to manage their identity and finances in the Web 2.0 era, their ability to (re)take control of their digital data should not be overlooked, especially with the advent of new 3.0 technologies that now enable them to do so with complete confidence.

In short, the digital society needs blockchain infrastructures with a high degree of decentralization (public blockchains), and more flexible, less decentralized infrastructures (private and hybrid blockchains). Ultimately, it's not a question of confronting these technological variants, but rather of seeking to understand them in order to promote their complementarity and convergence, because

[1472] The European Central Bank (ECB) has published a scientific article on its website, giving an idea of the extent of its political stance against the proof-of-work (PoW) computing mechanisms used by the Bitcoin protocol.) while a hands-off approach by public authorities is possible [regarding PoW], it is highly unlikely, and political action by authorities (e.g. disclosure requirements, a carbon tax on crypto transactions or holdings, or an outright ban on mining) is likely. ", MITSU Adachi, et al., "Stablecoins' role in crypto and beyond: functions, risks and policy", 2022, in *European Central Bank*, available at.

their different levels of decentralization simply respond to the different decentralization needs of society. While not everything can be decentralized, everything can be made more transparent. In this way, this research contributes to putting an end to the ideological dressing up that each of these technological variants undergoes. Nevertheless, the thrust of our study shows that private and hybrid blockchains are more suitable than public blockchains for implementing decentralized digital identity solutions in the short to medium term. This is due to their low cost per transaction, planned regulatory compliance and greater interoperability with conventional IT systems and use cases (1.0 and 2.0). This is borne out by the choice of this type of infrastructure for multiple European consortia such as the forthcoming European blockchain (EBSI), Spanish blockchain (Alastria), and French blockchain (Alliance Blockchain France). It is important to stress that in the event of a state implementing its own private blockchain, as in Estonia, it is advisable, as with any new technology, to adopt heightened vigilance in order to rule out any algocratic governance, i.e. any drift concerning the use of these 3.0 technologies (mass control or surveillance, dictatorship by the numbers)[14731474] . Ultimately, this study underlines the likelihood that private and hybrid blockchains will coexist with public blockchains, or even merge in the long term. Such a merger would only be possible if public blockchains deliver on their promises of resilience, energy efficiency and IT scalability, while anticipating the potential quantum supremacy (4.0) studied.

With regard to these 4.0 and 5.0 technologies, which are only mentioned in passing, but in anticipation of technology, we must not underestimate their potential to become fundamental issues in the future, given their potential to evolve over the coming years. Faced with the advent of all these new, interlocking technologies, we need to adopt a critical, yet objective, stance towards them. This means regularly and methodically challenging them in their conceptual and IT components, in order to gain a precise understanding of their consequences, and particularly of the legal rules governing them. This study confirms that every new technology is nothing more than a new medium and tool at people's disposal, whose use and subjective aims have dual effects for society as a whole. Lawyer and professor

[1473] CLAESSENS Michel, "Science et communication, pour le meilleur ou pour le pire?", chap. La dictature du chiffre, Éd. Quæ, 2009, pp.103-141.

[1474] De FILIPPI Primavera, "When controlled by a centralized, authoritarian government, the distinctive features of a blockchain - in terms of resilience, resistance to tampering and automatic execution - could lead to situations where powerful actors decide to incorporate their own set of rules into a blockchain-based system, so that anyone wishing to interact with that system will have no choice but to comply with those rules. This could ultimately help extend the power of rigid, authoritarian regimes, which would gain a greater ability to control their citizens through a set of self-executing, code-based rules," in *Blockchain and the Law*, *op. cit. by* Kinde, location 3973 of 7004.

Alain Supiot of the Collège de France believes that "*the problem is to know how to put our tools at our service instead of thinking that we are made on the model of our tools*"[1475] .

If new technologies are, in fact, nothing more than tools at the service of mankind, then it is as much the individual's responsibility as it is the collective's to ensure that technologies are used with respect for individual rights and freedoms, and that the development of information technology serves the common good. In this respect, the now inescapable subject of the energy impact and social utility attributed to 3.0 technologies must not be ignored by the players in these technological ecosystems. On the contrary, it needs to be examined in depth, with a scientific pragmatism coupled with a diversity of viewpoints, to become a priority. In fact, their future depends on the societal acceptance that will gradually be attributed, or not, to the specific cost/benefit ratio of each 3.0 technology. As regards both the energy footprint of IND's solutions, which process large volumes of data, and the energy impact of public blockchains and their crypto-assets, it will take a long time to reach reliable, objective conclusions. In conclusion, we need to adopt an optimistic and confident outlook on the future, on the grounds that the issue of defending and asserting digital rights has never been dealt with as much as it is today, and that these new 3.0 technologies are helping to strengthen people's rights online. The more citizens regain control of their identity and financial data, i.e., understand their importance, the more this awakening of the digital society will impose itself on major technology companies and governments, who will have to accept that these digital identities no longer belong to them. It is thus possible that technological choices will be imposed by the 3.0 needs and uses of these digital markets, dictated by Internet users, and not by the established powers, so that in the end "*we resist the invasion of armies, we don't resist the invasion of ideas*"[1476] .

***

[1475] CNNum, "Compte-rendu d'un échange avec Alain Supiot, professeur au Collège de France", published September 24, 2021, in *cnnumerique.fr*, accessed March 29, 2021.
[1476] HUGO Victor, "Histoire d'un crime, deposition d'un témoin", text prepared by J.M. Hovasse and G. Rosa, available at p.592.

Bibliography

I - Laws, legal acts, case law and doctrine

1.1 Laws, articles of laws, ordinances and other legal acts

Art. L102 of the French Post and Electronic Communications Code, Légifrance, available online

Déclaration des Droits de l'Homme et du Citoyen de 1789, Conseil constitutionnel, available at the following address

Code de la consommation, Livre Ier: information des consommateurs et pratiques commerciales, art. L111-1 to L141-2, Légifrance, available at the following address

Code civil, Art. 1188, Légifrance, available at Code civil, Art.

2061, Légifrance, available at

Code of Civil Procedure, Chapter I: Jurisdiction, art. 33 to 41, Légifrance, available at the following address

Penal Code, Art. 226-4-1 - Légifrance, available at the following address

French Monetary and Financial Code, Art. L54-10-1, Légifrance, available at the following address

Law of August 8, 1893 on the residence of foreigners in France and the protection of national labor, available at the following address

Law no. 72-3 of January 3, 1972 on filiation, available at the following address

Law no. 2000-230 of March 13, 2000 adapting the law of evidence to information technologies and relating to electronic signatures, available at the following address

Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (1), (LOPPSI), JORF n°0062 du 15 mars 2011, available at the following address

Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (1), (PACTE), JORF n°0119 du 23 mai 2019, available at.

Law no. 2023-171 of March 9, 2023 containing various provisions adapting to European Union law in the fields of the economy, health, labor, transport and agriculture, (DDADUE), JORF no. 0059 of March 10, 2023, available at the following address

Order no. 2005-1516 of December 8, 2005 on electronic exchanges between users and administrative authorities and between administrative authorities. Available at the following address

Ordinance no. 2016-131 of February 10, 2016 reforming contract law, the general regime and proof of obligations, available at.

1.2 Decrees

Ministerio del interior, Real Decreto 1553/2005, de 23 de diciembre, por el que se *regula la expedición del documento nacional de identidad y sus certificados de firma electrónica*, 2005, available at the following address

Decree no. 2022-1212 of September 2, 2022 concerning the entry into force of law no. 2022-300 of March 2, 2022 aimed at reinforcing parental control over Internet access.

Decree no. 2022-1620 of December 23, 2022 on the signing of declarations of company formalities, consultation of the National Register of Companies and the deregistration of certain companies.

Decree no. 2023-63 of February 3, 2023 on the verification of customer identity for certain products and services with a low risk of money laundering and terrorist financing.

1.3 Bylaws

Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé "FranceConnect", Légifrance, available at the following address

1.4 EU regulations

Regulation (EU) **No. 910/2014** of the European Parliament and of the Council of July 23, 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, or **eIDAS (Electronic IDentification And trust Services)**. Available at the following address

Commission Implementing Regulation (EU) **No. 2015/1502** of September 8, 2015 laying down minimum technical specifications and procedures relating to guarantee levels for means of electronic identification referred to in Article 8(3) of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Available at the following address

Regulation (EU) **No. 2016/679** of the European Parliament and of the Council of April 27, 2016, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) or **GDPR (General Data Protection Regulation)**. Available at the following address

Proposal for Regulation (EU) **No. 2020/0265** of the Parliament and of the Council of September 24, 2020 on markets in crypto-assets and amending Directive (EU) 2019/1937 or **MiCA (Market in Crypto- Assets)**. *(Not promulgated as of 15/04/2023)*. Available at the following address.

Proposal for Regulation (EU) **No. 2020/0340** of the European Parliament and of the Council of November 25, 2020 on European data governance (Data Governance Act) or **DGA**. Available at the following address

Proposal for Regulation (EU) **No. 2020/0374** of the European Parliament and of the Council of December 15, 2020 on fair and contestable contracts in the digital sector (digital market legislation) or **DMA (Digital Market Act)**. Available at the following address

Proposal for Regulation (EU) **No 2021/0136** of the European Parliament and of the Council of June 3, 2021 amending Regulation (EU) No 910/2014 as regards the establishment of a European framework for a digital identity or **eIDAS-2 (Electronic IDentification And trust Services)**. Available at the following address

Proposal for Regulation (EU) **No. 2021/0241** of the European Parliament and of the Council of July 20, 2021 on information accompanying transfers of funds and certain crypto-assets (recast) or **TFR (Transfer of Funds Regulation)**. *(Not promoted as of 15/04/2023)*. Available at the following address

Proposal for Regulation (EU) **No 2022/0032** of the European Parliament and of the Council of February 8, 2022 establishing a framework of measures to strengthen the European semiconductor ecosystem (Semiconductor Regulation). Available at the following address

Proposal for Regulation (EU) **No 2020/0047** of the European Parliament and of the Council of 23 February 2022 establishing harmonized rules for fairness in the access to and use of data (Data Regulation) or **Data Act**. Available at the following address

Regulation (EU) **No 2022/858** of the European Parliament and of the Council of May 30, 2022 on a pilot scheme for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU (text with EEA relevance) or **Régime Pilote DLT (Distributed Ledger technology)**. Available at the following address

Regulation (EU) **No 2022/2065** of the European Parliament and of the Council of October 19, 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation) or **DSA (Digital Service Act)**. Available at the following address

1.5 Guidelines

Directive (EU) **95/46/EC** of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at the following address

Directive (EU) **2015/849** of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive 2005/60/ec of the European Parliament and of the Council and Commission Directive 2006/70/ec. Available at the following address

Directive (EU) **No. 2015/2366** of the European Parliament and of the Council of November 25, 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC. Available at the following address

Directive (EU) **2019/1024** of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). Available at the following address

1.6 Case law and doctrine

ACPR (FLICHE olivier, URI Julien, VILEYN Mathieu), *Finance "décentralisée" ou "Disintermediation: the regulatory response*, discussion paper, April 2023. Available at the following address

EC, *La Commission propose une identité numérique fiable et sécurisée*, Press release of June 3, 2021, available at

CEF Digital, *eIDAS-Node Demo Tools Installation and Configuration Guide v2.6 (pre-release)*, 2021, available at

CJEU, *A contract for the provision of telecommunication services containing a clause according to which the customer has consented to the collection and storage of his identity document cannot demonstrate that he has validly given his consent where the relevant box was ticked by the data controller before the contract was signed*, on *Press Release No. 137/20*, Judgment in Case C- 61/19 Orange România SA/Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP), November 11, 2020, available at.

CNIL, *European Data Protection Regulation: what's changing for professionals*, available at

CNIL, *Sanctions (RGPD)*, available at the following address. CNIL, *Sanctions (RGPD)*, 2011-2023, available at the following address

CNIL. *Cookies: CNIL urges private and public organizations to audit their websites and mobile applications*, 2021, available online

Commission d'enrichissement de la langue française**,** *Vocabulaire des actifs numériques (liste de termes, expressions et définitions adoptés)*, JORF, no 13, 15 janv. 2021.

Commission staff working document impact assessment report accompanying the document proposal for a regulation of the European Parliament and of the Council amending regulation (eu) n° 910/2014 as regards establishing a framework for a european digital identity, available at the following address

COUNCIL OF EUROPE (G'SELL Florence, MARTIN-BARITEAU Florian), *The impact of blockchains on human rights, democracy and the rule of law*, 2022, available at.

CONSEIL DE L'EUROPE et CRID (POULLET Yves et DINANT Jean-Marc), *Comité consultatif de la convention pour la protection des personnes a l'égard du traitement automatisé des données à caractère personnel (t-pd) rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications l'autodétermination informnelle à l'ère de l'internet*, 2004, available at the following address

CONSEIL D'ÉTAT, *Annual study 2014 - Digital technology and fundamental rights*, available at

DALLOZ, *Lexique des termes juridiques*, 2017-2018, available at

European Data Protection Board, Article 29 Working Party, 2018, available at

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, June 20, 2007, available at

OHCHR, *International Covenant on Civil and Political Rights*, 1976, available at Humanium, *Geneva*

Declaration on the Rights of the Child, 1924, available at IAPP (DESAI Anokhy), *US State Privacy*

Legislation Tracker, available at

Notaires de France. *Le numérique, accompagner et sécuriser L'Homme. The digital revolution and the law*, 117ème Congrès des Notaires de France, 2021, Presentation available at and Report (*Chapter I - The development of the cryptoeconomy*) available at

WIPO, Summary of the Berne Convention for the Protection of Literary and Artistic Works (1886), available at

European Parliament. *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?* European Parliament study, Panel for the Future of Science and Technology.Scientific Foresight Unit (STOA). EPRS | European Parliamentary Research Service, 2019, available at

LCB-FT regulations: summary of the main measures to be implemented b y digital asset service providers, available at the following address

ROLLAND Paul, *Les Modes Alternatifs de Règlement des Différends (MARD) : à chacun sa voie*, on Village de la Justice. 2020. Available at the following address

U.S. Government Publishing Office, *Biometric identifiers and the modern face of terror: new technologies in the global war on terrorism, hearing before the subcommittee on technology, terrorism, and government information of the committee on the judiciary united states senate one hundred seventh congress*, first session, november 14, 2001. Available at the following address

UNICEF, *International Convention on the Rights of the Child*, 1990, available at

Working Party 29, *Opinion 3/2012 on the evolution of biometric technologies*. Available at the following address

Court of Cassation, Civil, Civil Division 1, November 3, 2016, 15-22.595, Published in the bulletin | La base Lextenso, available online.

CNIL, *Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail*, Légifrance, available at.

CA de Montpellier, Civ. 2ème ch., October 21, 2021, N°RG 21/00224, in *Actualité Droit Propriété Intellectuelle Technologie de l'information Innovation* - Cabinet Simon et Associés Avocats, available at the following address

II - Books and book chapters

AÏDAN Geraldine, **DEBAETS Emilie***, L'identité juridique de la personne humaine,* ed. L'Harmattan, coll. Logiques Juridiques, 2013.

ALFORD Richard D, *Naming and identity: a cross-cultural study of personal naming practices*, HRAF Press, 1988.

AMMOUS Saifedean, *The Bitcoin Standard*, ed. Dicoland (LMD), 2019.

ANTONOPOULOS Andreas, *Mastering Bitcoin 2nd Edition*, ed. O'Reilly Media, 2015.

ANTONOPOULOS Andreas, *The Internet of Money,* ed. Kindle, 2016.

AZAN Wilfrid, CAVALIER Georges, *Des systèmes d'information aux blockchains*: *Convergence en sciences juridiques, fiscales, économiques et de gestion*. Larcier, coll. Droit et économie, 2021.

BELLANGER Pierre, *La souveraineté numérique*, ed. Stock, 2014.

BERGER Peter, **LUCKMANN Thomas**, *La construction sociale de la réalité*, Ed. Armand Colin, coll. Individu et Société, 2018.

BERNARD Alain, *L'identité des personnes physiques en droit privé : Remarques en guise d'introduction*, p. 29.

BERTHOZ Alain, **DEBRU Claude**, *Anticipation and prediction: from gesture to mental journey*, Odile Jacob, 2015.

BISMUTH Yves, *Le droit de l'informatique*, ed. L'Harmattan, 4th edition, 2017.

BLONDIAUX Loïc, **KANTOROWICZ Ernst***, Les deux corps du Roi*, ed. Gallimard, 1989, Politix. Revue des sciences sociales du politique, 2, Persée - Portail des revues scientifiques en SHS, 1989, nº 6,
p. 84-87, available at

BOUILLET-CORDONNIER Ghislaine, **MOULIN Jean-Marc**, **QUINIOU Matthieu**, **GASSER Axel et al**. *La finance numérique: aspects juridiques et fiscaux du crowdfunding et des cryptoactifs*, Ed. EFE, 2021.

CATALA Pierre, *Le droit à l'épreuve du numérique : jus ex machina*, 1st edition, PUF, coll. Droit, éthique, société, 1998.

CONSTANT Benjamin, *De la liberté des anciens comparée à celle des modernes*, ed. Mille et une nuits, coll. 1001 Nuits Petite Collection, 2010.

COTIGA-RACCAH Andra, **JACQUEMIN Hervé**, **POULLET Yves**, *Les blockchains et les smart contracts à l'épreuve du droit*, 1éd. Larcier, coll. CRIDS, 2020.

CRETTIEZ Xavier, **PIAZZA Pierre**, *Du papier à la biométrie. Identifying individuals*, Sciences Po Presses, 2006.

CRUET Jean. *The moral and social philosophy of Destutt de Tracy (1754-1836) / Jean Cruet*. BNF/Gallica. 1909.

De FILIPPI Primavera, WRIGHT Aaron, *Blockchain and the Law: The Rule of Code*, ed. Harvard University Press, 2018.

DESCOMBES Vincent, *Les embarras de l'identité*, ed. Gallimard, coll. NRF Essais, 2013.

DUBAR Claude, *La crise des identités, l'interprétation d'une mutation*, ed. PUF, coll. Le lien social, 2010.

DUMA Jean, *Norbert Elias and La Société des individus*, *Histoires de nobles et de bourgeois: individus, groupes, réseaux en France. XVII et XVIII siècles*, Nanterre, Presses universitaires de Paris Nanterre, 2016, p. 17-31. Available at

DURKHEIM Émile, *Education and sociology*, ed. PUF, coll. Quadrige, 2013.

DURKHEIM Émile, *Leçons de sociologie. Physique des mœurs et du droit*, 157p.

EYNARD Jessica et al. *L'identité numérique ; quelle définition pour quelle protection ?* Ed. Larcier, coll. Création information communication, 2020.

FAVIER Jacques. **LECRIVAIN Jean-Samuel** and **TAKKAL-BATAILLE Adli**, *Bitcoin et protocoles à blockchain. Comprendre l'avènement de la seconde ère numérique*, Mardaga, coll. "Gestion, Entreprise, Finance", 2019.

FRUMKIN Daniel, *Bitcoin Mining Handbook*, ed. Braiins Publishing, 2022.

FUNES (de) Julia, *Quand l'identité devient un piège*, ed. La Montagne, 2023.

GARAPON Antoine and **LASSEGUE Jean**, *Justice digitale: révolution graphique et rupture anthropologique*, PUF, 2018.

GAYON Jean, **NICOGLOU Antoine**, **PONTAROTTI Gaëlle et al**. *L'Identité*. Dictionnaire encyclopédique Gallimard. Folio Essai, 2020.

GUILLAUME Florence, **MAHON Pascal**, *Le droit à l'intégrité numérique: réelle innovation ou simple évolution du droit?* Helbing Lichtenhahn Verlag, 2021.

GUILLAUME Florence, **MAHON Pascal**, **ROUSSEL Alexis et al**. *Réelle innovation ou simple évolution du droit? le droit à l'intégrité numérique*, Université de Neuchâtel, Éd. Helbing, Lichtenhahn, 2020.

ITEANU Olivier, *Quand le digital défie l'Etat de droit*, ed. Eyrolles, 2016.

ITEANU Olivier, **SALVATORY Olivier**, *L'identité numérique en question: 10 scénarios pour une bonne gestion juridique de son identité sur internet*, ed. Eyrolles, 2008.

JEAN Aurélie, *Do algorithms make the law?* Ed. de l'Observatoire, 2021.

KAKU Michio (author), **DEPOVERE Paul** (translation), *L'avenir de l'humanité*, ed. De Boeck Supérieur, coll. Hors collection Sciences, 2019.

KHATCHATOUROV Armen, *Digital identities in tension. Between autonomy and control*, 2019, ISTE Editions.

KLUMOV Gregory, *Digital asset regulation. a cross-country analysis*, 2019.

KUNDERA Milan, *L'identité*, ed. Gallimard, 1998.

LANGLOIS-BERTHELOT Thibault et al. *La Finance Numérique: aspects juridiques et fiscaux du crowfunding et des cryptoactifs*, EFE Edition, pp.147-151, 2021, available at

LANGLOIS-BERTHELOT Thibault et al. *Legal perspectives on the emergence of a decentralized identity in the service of augmented digital rights*. In *Blockchain et Cryptos | 60 experts explain it all*, IS EDITION, pp.516, 2022, Wallcrypt, Chapter available at

LASSEGUE Jean, **GARAPON Antoine**, *Justice digitale*, PUF, 2018.

LEGEAIS Dominique, *Blockchain and digital assets*, LexisNexis, coll. "Actualité", 2019.

LOCKE John. *Property: John Locke, Second Treatise, Chap. 16 §§ 25--51, 123--26,* 1689.

LOISEAU Grégoire, *Droit des personnes - 2e édition mise à jour et augmentée*, Ed. ELLIPSES, May 12, 2020.

LOISEAU Grégoire, *Précis de culture juridique* (ed. F.-X. Lucas and T. Revet), 6th edn, 2022, p.135.

LOURIMI Alexandre, BARBET-MASSIN Alice, O'RORKE William, PION Claire, FLEURET Faustine, *Droit des crypto-actifs et de la blockchain*, ed. LexisNexis, 2020.

MAALOUF Amin, *Les identités meurtrières*, ed. Grasset, 1998.

MAUSS Marcel, *La Nation*, ed. Minuit, 1920, available at

MONEGER Françoise, *Droits de l'enfant*, ed. DALLOZ, 2017.

MOROZOV Evgeny, *Pour tout résoudre, cliquez ici : l'aberration du solutionnisme technologique*, Fyp éditions, 2014.

MUCCHIELLI Alex, *L'identité*, ed. Presses Universitaires de France, coll. Que sais-je? 2009.

NISSENBAUM Helen, *Privacy in context: technology, policy, and the integrity of social life*, Stanford University Press, 2009, p. 304

NOIZAT Pierre, *Bitcoin Book*, Kindle ed., 2012.

NOIZAT Pierre, *Bitcoin, mode d'emploi*, ed. Lulu.com, 2015.

PIKETTY Thomas, *Le capital au XXIe siècle*, Ed. Seuil, coll. les livres du nouveau monde, ISBN: 978.2.02.108228.9, 2013.

PREUKSCHAT Alex, **REED Drummond**, *Self-Sovereign Identity: decentralized digital identity*, publication start December 2019 and final publication summer 2020, ISBN 9781617296598.

RADLEY-GARDNER Oliver, **BEALE Hugh** and **ZIMMERMANN Reinhard** (eds.), *Fundamental Texts On European Private Law*, Hart Publishing, 2020.

REY Olivier, *Leurre et malheur du transhumanisme*, ed. Les Carnets DDB, 2020.

RICOEUR Paul, *Soi-même comme un autre*, Ed. Seuil, 1990.

SIMMEL Georg, *Philosophy of Money*, ed. Quadrige, 2014.

STACHTCHENKO Alexandre, **BALVA Claire**, *Bitcoin & cryptocurrencies made easy - understanding digital currencies and their economic challenges*, EAN13: 9782412081716, First publisher, 2022.

STACHTCHENKO Alexandre, BALVA Claire, JEANNEAU Clément, YERETZIAN Antoine, *La blockchain décryptée - les clefs d'une révolution*, ed. Netexplo, 2016.

STIEGLER Bernard, *L'attention, entre économie restreinte et individuation collective*, ed. L'économie de l'attention: Nouvel horizon du capitalisme?, 2014, pp. 121-135.

SUPIOT Alain, *Homo juridicus: essai sur la fonction anthropologique du droit*, Seuil, 2005.

SUPIOT Alain, *Governance by numbers*. Cours au Collège de France (2012-2014), Coll. Poids et mesures du monde, Ed. Fayard, 2015.

TAPSCOTT Alex, **TAPSCOTT Don**, *How the technology behind Bitcoin is changing money, business, and the world in Blockchain revolution*, ISBN 9781101980132.

TELLER Marina, *The advent of Deep Law (towards a digital analysis of law?)*, 2020.

TOCQUEVILLE Alexis, *Le despotisme démocratique*, ed. L'HERNE, 2009.

ZUBOFF Shoshana, *The age of surveillance capitalism*, Kindle ed., 2019.

III - Dissertations and theses

ALSAEDI Musabbeh. *The United Arab Emirates and the digital revolution. New challenges for public, private and criminal law*. Doctoral thesis in law. Université Paris I Panthéon- Sorbonne

BARBET-MASSIN Alice. *Le droit de la preuve à l'aune de la blockchain*. Doctoral thesis in law. University of Lille, 2020, available at

CONSTANTINO FERREIRA Leonel. *Blockchain dispute resolution. Towards decentralized arbitration?* Master's thesis, University of Neuchâtel, 2021, available online

DIOP Mame Mariama. *Securing the payment services market*. Doctoral thesis in law. University of Lille, 2015, available online

DOERK, Adrian. *The growth factors of self-sovereign identity solutions in Europe*. Bachelor Thesis. 2020. Available at

EDDEROUASSI Meryem. *Le contrat électronique International*, PhD thesis in law. Université Grenoble Alpes, 2017, available online

ELIE Pauline, *Analyser l'identité en droit : comment protéger et définir un nouveau territoire à l'ère dématérialisée ?* v. Thesis in progress at EHESS, available at the following address

FOUQUET Kévin, *L'état civil sénégalais aujourd'hui de l'enregistrement à l'archivage*, Mémoire Master 1, 2020, Université d'Angers, available at

GASSER Axel, *Le financement alternatif de la transition énergétique (aspects juridiques)*, dissertation project in Private Law under the supervision of Jean-Marc Moulin, University of Perpignan.

GUILLEBON Thibaud. *Les monnaies virtuelles: essai sur l'intégration d'une nouvelle classe d'actifs dans les concepts fondamentaux du droit privé*, University of Bordeaux, 2022, available online

HOANG Van-Hoan. *Securing data access and exchanges in a heterogeneous ecosystem: An adaptive and context-sensitive approach*. Cryptography and Security Thesis. University of La Rochelle, 2022. English. Available at the following address

JULIEN Marine. *Digital trust in banking*. Doctoral thesis in law. University of La Rochelle, 2022, available at the following address

LANGLOIS-BERTHELOT Thibault. *Les méthodes de légalisation et de blanchiment des activités mafieuses*, Master 2 thesis, Université Paris Nanterre & EHESS, available at the following address

LASSEGUE Jean, *L'intelligence artificielle et la question du continu; Remarques sur le modèle de Turing*, Thesis in Philosophy, Université de Nanterre - Paris X, 1994, available at

LEE David. *Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups*, University of California, 1982, available at

LEHMAN Constance. *Essay on price and value in contract law*. Doctoral thesis in law. Université Paris-Saclay, 2022. French. Available online

LEVENEUR Claire. *Smart contracts: a study of contract law in the light of blockchain.* Thesis in law. Université Paris 2, 2022, available at

LOPAMUDRA Mandal, *Ricardian contract: Bridging the Gap Between Smart Contracts and Traditional Contracts*, Master Thesis, International Business Law, June 2019, p.10, available online at.

SZTULMAN Marc. *Biométrie et libertés : contribution à l'étude de l'identification des personnes*, PhD thesis in law, Université Toulouse 1, 2015, available at.

IV - Magazine and newspaper articles

ALLISON Arthur, **CURRALL James E. P**, **MOSS Michael**, **STUART Susan**. *Digital identity matters*, 2005, Journal of the American society for information science and technology. Available at the following address

AMR Jacques, PASQUALINI François, De VAUPLANE Hubert et al, *Dettes de l'Etat, dettes des entreprises: quel avenir?* Ed, Bruylant, coll. Droit & Economie, 2023.

ANCIAUX Arnaud, **FARCHY Joëlle**, *Données personnelles et droit de propriété : quatre chantiers et un enterrement*, Revue internationale de droit économique, November 2015, nº 3, p. 307-331, available at.

BARBET-MASSIN Alice, *Réflexions autour de la reconnaissance juridique de l'horodatage blockchain par le législateur italien*, Revue Lamy droit de l'immatériel (WoltersKluwer), n°157, 2019.

BELGA. *Des algorithmes plus transparents : l'UE va les réclamer à Facebook et Google*, on *RTBF Info*, 2020, available at the following address

BENOÎT-GUILBOT Odile, **EVERETT Rogers**, *Diffusion of innovations*, Revue française de sociologie, 5, Persée - Portail des revues scientifiques en SHS, 1964, nº 2, p. 216-218. Available at the following address

BERTRAND-MIRKOVIC Aude, *La notion de personne,* Presses universitaires d'Aix-Marseille, 2003.

BOULLIER Dominique, *Puissance des plateformes numériques, territoires et souverainetés*, Sciences Po, Centre d'Etudes Européennes et de Politique Comparée, 2021, available at

BOUSQUET Marc, *Tout savoir sur le Bitcoin et les cryptomonnaies*, Dossiers Science Hors-Série, Sens edition, ISSN: 2802-1843, 2022, 65 pages.

BUTERIN Vitalik, *On Nathan Schneider on the limits of cryptoeconomics*, online article, 2021, available at

BUTERIN Vitalik, *The Limits to Blockchain Scalability*, online article, 2021, available at.

CARDON Dominique, *L'identité comme stratégie relationnelle*, Hermes, La Revue, n° 53, 2009, nº 1, p. 61-66, available at

CEYHAN Ayse, *Lutte contre le terrorisme : la technologie n'est pas neutre*, Revue internationale et stratégique, n° 74, juin 2009, nº 2, p. 18-27, available at

CHAMBARDON Nicolas, *L'identité numérique de la personne humaine. Contribution à l'étude du droit fondamental à la protection des données à caractère personnel*. PhD thesis in law, Université Lumière-Lyon-2, Revue des droits et libertés fondamentaux, 2019, abstract available at

CHARDEL Pierre-Antoine, DARTIGUEPEYROU Carine, *Être, temps et différences : pour une approche différencialiste du temps à l'ère numérique*, 2018, Ed. Nicole Aubert, in *la recherche du temps: Individus hyperconnectés, société accélérée : tensions et transformations*, pp. 95-110.

CHARDEL Pierre-Antoine, *L'éthique dans la société technologique : un défi pédagogique majeur*, 2014, Ed. Edwige Rude-Antoine, in *Un état des lieux de la recherche et de l'enseignement en éthique*, l'Harmattan, pp. 131-146.

COROT Léna. *Apple attacks Zoom and Teams and unveils a digital identity wallet*, on *Usine-digitale.fr*. 2021. Available at

De MOMBYMES Yorick, *Anarchy, cypherpunk and freedom: the philosophical roots of bitcoin*, in Contrepoints.org, March 17, 2018. Available at

De VAUPLANE Hubert, *What regulation for cryptocurrency public offerings (ICOs)?* Revue Banque, n°810, 2017.

From VAUPLANE Hubert. *Will blockchain defy the rule?* RDBF, n°6, 2016, p.115.

DEFFAINS Bruno, *Blockchain - Pour un open source responsable!* in *Lexisnexis*, La semaine du droit n° 14, April 6, 2021, available at

DOUVILLE Thibault, *Blockchains and evidence*, Ed. Dalloz, 2018.

DUPUY, Caroline. *Cryptomonnaies : comment ça marche ?* Les Nouvelles Publications. 2018. Available at

EGE Ragip, *À propos de l'ouvrage de Karl Marx: contribution à la critique de l'économie politique. Introduction aux Grundrisse dite" of 1857*, Cahiers d'économie Politique, no. 70, October 2016, nº 1, p. 163-166, available at

FERRIÉ Scarlett-May, *Le droit à l'autodétermination de la personne humaine: essai en faveur du renouvellement des pouvoirs de la personne sur son corps*, IRJS éditions, 2018.

FERRY Luc. *La fin de l'individu, vraiment?* on *LEFIGARO*, published on October 23, 2019, available at

France Culture. *Heraclitus, you never enter the same river twice - Ep. 1/4 - Anything new?* 2017. Audio series available at

GEORGES Fanny, *Représentation de soi et identité numérique*, Réseaux, n° 154, April 2009, nº 2, p. 165-193, available at

Id, *Le design de la visibilité*, Réseaux, n° 152, 2008, nº 6, p. 93-137, available at

JEAN Aurélie, *Pourquoi Facebook doit rester en dehors du métavers*, on *Le Point*, 2021, available at

KLIPPENSTEIN Ken and **SIROTA Sara**, *The Taliban Have Seized U.S. Military Biometrics Devices*, on *The Intercept*, 2021, available at

KOENIG Gaspard, *La propriété de soi*, Revue des juristes de sciences po - n°17 - juin 2019, available at

KRYPTOSPHERE®. *KryptoPaper: Blockchain & crypto*, 2022, on LinkedIn, available at

LARDELLIER Pascal, **BRYON-PORTET Céline**, *Ego 2.0*, Les Cahiers du numérique, Vol. 6, July 2010, nº 1, p. 13-34, available at

LASSEGUE Jean, *Le droit automatisé et le problème de la délibération collective*, Dalloz IP / IT Droit de la propriété intellectuelle et du numérique Numéro 1 - Janvier 2022, Dossier, p. 12. *Justice par la Blockchain*, available at.

LE HEN Solène. *Three questions about the new identity card that comes into force on Monday August 2*, on *Franceinfo*, published August 2, 2021, available at

LEGEAIS Dominique. "L'apport de la Blockchain au droit bancaire", RDBF, Jan. 2017, p. 5.

LOW Kelvin F.K., **MIK Eliza**, *Pause the Blockchain Legal Revolution*, Aug. 22, 2019, reviewed Apr. 6, 2020, in International & Comparative Law Quarterly 135-175, available at.

MAUGER Gérard. *A. Strauss, Miroirs et masques. An introduction to interactionism*, in Politix, vol. 6, n°21, 1er trimestre 1993. Représentations de Paris. pp. 142-146, available at

MESURE Sylvie, *Le lien social à l'épreuve de l'individualisme le " culte de l'individu chez Durkheim "*, Revue internationale de philosophie, n° 280, avril 2017, no 2, p. 157-180, available at.

MIRHADY David C., *Aristotle and the Law Courts*, in Polis: The Journal for Ancient Greek Political Thought, 23, 2006, no 2, p. 1/17, available at

MOEREL Lokke and **TIMMERS Paul**, *Reflections on Digital Sovereignty*, on EU Cyber Direct, 2021, available at

NAKAMOTO Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Oct. 31, 2008, available at

NEWTON Casey, *Mark Zuckerberg is betting Facebook's future on the metaverse*, on *The Verge*, July 22, 2021, available at.

NOUR Soraya and **LAZZERI Christian**, *L'intégration parreconnaissance del identité : l'héritage freudien*, on Presses universitaires de Paris Nanterre, 2009, available at

PARGAMIN David, *Les réseaux sociaux font payer la fin de l'anonymat*, Revue Challenges n° 776, March 2, 2023, p. 34 and 35.

PARGAMIN David, *Sur la piste des voleurs de cryptomonnaies*, Revue Challenges n°779, March 23, 2023, p. 46 and 47.

PARK Sunoo, **SPECTER Michael**, **NARULA Neha**, **RIVEST Ronald L**. *Going from Bad to Worse: From Internet Voting to Blockchain Voting*, MIT, 2020, available at.

PELLEGRINI François, **VITALIS André**, *La création du fichier biométrique TES : la convergence de logiques au service du contrôle*, Sociologie, PUF, December 2017, no N° 4, vol. 8, available at.

PERRET Virgile, *Monnaie et citoyenneté : une relation complexe en voie de transformation*, on International Studies, 2011, available at

SPIVAC Simon, *Claude Lévy-Strauss, La pensée sauvage*, Revue Tiers Monde, 5, Persée - Portail des revues scientifiques en SHS, 1964, no 19, p. 596-597, available at

SUBTIL Romain. *Protection des données personnelles : la Californie s'inspire de l'Europe*, on *La Croix*, 2018, available at.

VERBIEST Thibault, *Technologies de registre distribué (blockchain) : premières pistes de régulation*, RLDI, no 129, 2016, p. 52.

WOITIER Chloé. *Facebook and Ray-Ban unveil their connected pair of glasses, the Ray-Ban Stories*, on *LEFIGARO*, published September 8, 2021, available at.

World Bank Group. *Cross-practice initiative: Identification for Development*. Flyer, 2015, available at

WRIGHT Aaron, **De FILIPPI Primavera**, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015.

ZOLYNSKI Célia, *La place du règlement (UE) 2018/1807 dans la construction du droit des données de l'Union européenne*, Dalloz IP/IT, 2020.

V - Articles, studies, reports, videos and online pages

ABRAMOV Oleg, **BEBELL Kirstin L**. and **MOJZSIS Stephen J**. *Emergent Bioanalogous Properties of Blockchain-based Distributed Systems*, *in Origins of Life and Evolution of Biospheres*, 51, June 2021, nº 2, pp. 131-165, available at.

Académie Française. *Identity*, Dictionnaire de l'Académie française, available at the following address

ADAN and **KPMG**, *La crypto en France: structuration du secteur et adoption par le grand public*, 2022, available at

AFLALO Jérémie, **MILLERAND Arthur**, **LECLERC Michel**. *Le numérique peut-il sauver la démocratie?* on *Third* and *PARALLEL AVOCATS*, 2021, available at

Alliance pour la Confiance Numérique, *Collectif pour la Feuille de route Nationale sur l'identité numérique*, 2014, available at.

ANDERBERG, A. ANDONOVA, E. BELLIA, et al. Publications Office of the European Union, Luxembourg, 2019, available at

ANGELI Guillaume, **SFEZ Betty**, **CHOUTEAU Vincent**, **Broustail Alain** for SOLEGAL and Blockchain EZ White paper *The usefulness of electronic signature on public blockchain for major accounts: interest, feasibility and legal value*. 2020. Available at the following address

ANSSI. *Publication of the repository of requirements applicable to remote identity verification service providers (PVID),* on *ANSSI*, available at the following address

AUDRAND Stéphane. "*Conquérir ou soumettre" - reflections on the constraints of a "forced" reunification of Taiwan with the People's Republic of China*, on *Theatrum Belli*. 2021, available at the following address

BALL Matthew. *Framework for the Metaverse*, on *MatthewBall.vc*, 2021, available at

BAMDÉ Aurélien. *Informational self-determination*, on *A. Bamdé & J. Bourdoiseau*, available at

BAMDÉ Aurélien. *The attributes of the right of ownership: usus, fructus and abusus*, on *A. Bamdé & J. Bourdoiseau*, 2020, available at

BBC. *Apple digital IDs come with conditions and costs*, on *BBC News*. Available at the following address

BECKER Katrin. *Blockchain Matters-Lex Cryptographia and the Displacement of Legal Symbolics and Imaginaries*. Law and Critique. 2022. Available at

BECKER Katrin. *Blockchain technology and the crypto-divine promise to do away with third parties*. On Digital Studies, 2019. Available at.

BECKER Katrin. *Lex cryptographica, smart contracts and personalized governments: The legal-cultural implications of blockchain technology*. On Grief, available at

BLANDIN Apolline, **PIETERS Gina**, **WU Yue**, **et al**. *3rd Global Cryptoasset Benchmarking Study*, Cambridge Center for Alternative Finance, University of Cambridge Judge Business School, 2020.

BONAZZI Hervé, **HEUDEBERT Paola**, **DROUOT Quentin et al**. *The future of digital identity is decentralized*, 2021, available at

BOTHOREL Eric, **COMBES Stéphanie**, **VEDEL Ranaud et al**. *Mission Bothorel - Pour une politique publique de la donnée*, SIRCOM, Mission confiée par le Premier ministre, 2020.

BOUFFARTIGUE Jean, *Les animaux techniciens*, *Rursus. Poiétique, réception et réécriture des textes antiques*, Université Nice-Sophia Antipolis, July 2006, nº 1, available at the following address

BOUILLET-CORDONNIER Ghislaine, LANGLOIS-BERTHELOT Thibault, *Tour d'horizon du droit financier Suisse : Crowdfunding - ICO - STO*, *Albatross Legal*, 2021, available at

CAMERON Kim, *The Laws of Identity*, 2005, article available at the following address

CAMPESE Sandrine. *Voltaire, le jugleur de lettres (1/2)*, on *Le Projet Voltaire*, 2015, available at.

CARRICK, Jon. *Bitcoin as a Complement to Emerging Market Currencies*. Emerging Markets Finance and Trade, 2016. Available at

CARSON Brant, **ROMANELLI Giulio**, **WALSH Patricia**, **ZHUMAEV Askhat** for MCKINSEY. *The strategic business value of the blockchain market*, 2018, available at.

CARUGATI Christophe, *Building an efficient regulation in the digital economy*, on CRED, working paper n°2020-10.

Cercle du Coin. *Cercle du Coin Round Table: Proof of work and ecology*, available at the following address

CHAROLLES Valérie. *Distinguishing liberalism and capitalism in the 21st century* - S&O Center HEC Paris. 2020. YouTube. Available at the following address

CHM. *Internet History of 1980s | Internet History | Computer History Museum*, available at

CNIL. *Premiers éléments d'analyse de la CNIL - Blockchain*, 2018, available at.

CNIL. *Quand la confiance paie : les moyens de paiement d'aujourd'hui et de demain au défi de la protection des données*, 2021, available at the following address

COURBE Thomas et al. *Les verrous technologiques des blockchains*, Report for the Government by INRIA, CEA and ITM, 2021.

CROUSILLAC Jean, *Le Combat des Enfants Fantômes*, Backpack Productions, 2021, report available at the following address.

De COETLOGUON Perrine, **DURAND Marc**, **GENIN Claire**, **BOULET Pierre**, **LANGLOIS-BERTHELOT Thibault et al**. *Blockchain technologies serving the public sector*, 2021, Report available at.

De LA BOÉTIE Étienne, *Discours de la servitude volontaire*, available at

De LA RAUDIERE Laure and **MIS Jean-Michel**. *Rapport d'information* déposé en application de l'article 145 du Règlement en conclusion des travaux de la mission d'information commune *sur les chaînes de blocs (blockchains)*, Assemblée nationale, 2018, available at.

From MOMBYNES Yorick. *Depoliticizing currency*. YouTube Conference at Surfin' Bitcoin. 2022, available at the following address

Discover Bitcoin. Youtube channel available at the following address

DHAPTE Aarti, *Blockchain Identity Management Market Research Report Information by Component Type (Software, and Solution), by Provider (Application, Middleware, and Infrastructure), by Organization Size (Large Enterprises, and SMEs), by Vertical (BFSI, Telecom & IT, and Government), By Region (Asia-Pacific, North America, Europe, and Rest of the World) - Forecast till 2030*, 2023, analysis available at

DOMINGO Agnacio Alamillo, *SSI eIDAS Legal Report: How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market*, European Commission & CEF Digital Connecting Europe, 2020, available at

Europe Finances Régulation. *La confidentialité des paiements : du xviiie siècle à l'euro numérique*, Revue d'èconomie Financière, n.°149

European Union Blockchain Observatory & Forum, *EU Blockchain Ecosystem Developments*, 2020, available at

EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM *Legal and Regulatory Framework of Blockchains and Smart Contracts*, 2019.

EUROPEAN UNION BLOCKCHAIN OBSERVATORY AND FORUM. *Blockchain and Digital Identity*, 2019.

EUROSMART. *Eurosmart positionpaper post quantum cryptography*, 2021, available at the following address

EY-Parthenon. *Modèles économiques de l'identité numérique*, in acteurspublics.fr, 2019, available at

FAURE-MUNTIAN Valeria and **FASQUELLE Daniel**. *Rapport d'information* déposé en application de l'article 145 du Règlement en conclusion des travaux de la mission d'information commune *sur les plateformes numériques*, Assemblée nationale, 2020, available at

GAUDIAUT Tristan. *Infographie : L'informatique entre l'ère quantique*, on *Statista Infographies*, 2021, available at the following address

GEORGAKOPOULOS Takis for JP MORGAN, *Payments are eating the world*, 2021, available at

GHOSH Devarsi. *Meet 'Elliot Alderson' - the vigilante hacker taking down UIDAI, one tweet at a time*, on *Scroll.in*. 2018. Available at

GODEFROY Lemy D., **LEBARON Frédéric**, **LEVY-VEHEL Jacques**. *How digital technology is transforming law and justice towards new uses and an upheaval in decision-making*. Research report. Mission de recherche. Law and Justice. 2019. Available at the following address

Government. L'Agenda 2030 en FRANCE, *ODD16 - Promouvoir l'avènement de sociétés pacifiques et ouvertes aux fins du développement durable*, available at the following address

GRAMLICH John. *10 facts about Americans and Facebook*, on *Pew Research Center*, available at

Grand Angle Crypto. Youtube channel available at the following address

GREGOIRE Paul and **HILLS Adam**. *Digital Identity Theft and Online Fraud in NSW*. NSW Courts. 2020. New South Wales Courts. Available at

GRIGG Ian. *Financial Cryptography in 7 Layers*, available at

GRIGG Ian. *The Ricardian Contract*, available at

HAMILTON DUFFY Kim et al. *Building the digital credential infrastructure for the future,* A White Paper by the Digital Credentials Consortium, 2020, available at

HAO Karen. *How Facebook and Google fund global misinformation,* on *MIT Technology Review*, 2021, available at

HENNEBERT Christine, **Coutor Sophie, FAHER Mourad**. *Blockchain and digital identification - Restitution des ateliers du groupe de travail 'blockchain et identité'*, Rapport du Ministère de l'intérieur, 2020, available at.

HENNION Christine and **MIS Jean-Michel**. *Rapport d'information* déposé en application de l'article 145 du Règlement en conclusion des travaux de la mission d'information commune *sur l'identité numérique*, Assemblée nationale, 2020, available at

HEUDEBERT Paola, DROUOT Quentin, et al. *The future of digital identity will be decentralized*. Archipels White Paper, 2021, available at

HUBBARD Bryan, *Federally Chartered Banks and Thrifts May Participate in Independent Node Verification Networks and Use Stablecoins for Payment Activities*, on Office of the comptroller of the Currency, 2021, available at

HUGUES Eric. *A Cypherpunk's Manifesto*, on *Adam.nz*, 1993, available at

KRYPTOSPHERE®, *Ricardian contracts, the future of smart contracts?* on *Cryptoast*, published on September 5, 2020, article available at.

KRYPTOSPHERE®, *Milton Friedman predicted the air of crypto-currencies in 1999!* 2019. Youtube video, available at the following address

KRYPTOSPHERE®. *Discovering the cypherpunk movement behind Bitcoin*, on *Cryptoast*, 2020, available at

L'HERMITE Marie and **STENNE Paul**, *La preuve, la blockchain et les professions réglementées*, Nuäg, 2019, available at.

LAHER Rudy, *La numérisation des activités de l'huissier de justice*, *Cahiers Droit, Sciences & Technologies*, PUP, May 2020, nº 10, p. 129-145, available at

LANDAU Jean-Pierre and **GENAIS Alban**, *Les crypto-monnaies*, Report to the Minister of the Economy and Finance, 2018, available at.

LANGLOIS-BERTHELOT Thibault et al. Part: *Towards a decentralized digital identity*. Report 2021 from the Banque de France's Observatoire de la Sécurité des Moyens de Paiement (OSMP), available at

LANGLOIS-BERTHELOT Thibault. *Blockchain, a new foundation for digital trust?* Observatoire d'IN Groupe, 2021, article available at the following address

LANGLOIS-BERTHELOT Thibault. *Proposal for a French taxonomy for decentralized identity*. 2021. Available at the following address

LAROUSSE. *Identité bas latin identitas -atis from classical latin idem le même* - LAROUSSE, available at the following address

LAW COMMISSION (UK), *Smart legal contracts: advice to government*, 2021.

LEQUESNE-ROTH Caroline. *Taxation of NFTs and the Metaverse - An introduction*. Revue de droit fiscal, 2022, available at

LEQUESNE-ROTH Caroline. *Metavers, Web3 : la révolution juridique en trompe-l'oeil*. Receuil Dalloz, 2022. Available at the following address

LITAN Avivah. *Hype Cycle for Blockchain 2021; More Action than Hype*, 2021, article available at.

LOCKWOOD Mick. *An Accessible Interface Layer for Self-Sovereign Identity*, *Frontiers in Blockchain*, 2021, available at.

MARTINSON Priit for PWC. *Estonia -the Digital Republic Secured by Blockchain*, 2019. Available at

MICROSOFT. *Microsoft HoloLens | Mixed Reality Technology for Business*, 2022, available at

MRASILEVICI Christian. *Valérie Charolles, Se libérer de la domination des chiffres*. 2022. YouTube. Available at the following address

NAKAMOTO Satoshi. V. *Profile of satoshi*, on bitcointalk, available at

National Science & Technology Council. *NSTC National Strategic Overview for QUANTUM INFORMATION SCIENCE*, 2018, available at

United Nations, *Birth registration and the right of everyone to recognition everywhere as a person before the law*, General Assembly of March 19, 2013, Human Rights Council: Twenty-second session, available at.

United Nations, *General Assembly adopts ambitious Sustainable Development Agenda for the 21st century "Transforming our world" within 15 years* | UN Press (2015, September 25). Available online

NETTER Emmanuel. *Blockchain and the regulated professions. What place for the regulated professions in the digital revolution?* Colloquium organized by M. Blanchard and S. Moreil, 2018, available at

El MADHOUN Nour, HATIN Julien, BERTIN Emmanuel, *A Decision Tree for Building IT Applications What to choose: Blockchain or Classical Systems?* Annals of Telecommunications - annales des télécommunications, in Springer, 2021, available online

El MADHOUN Nour, MALDONADO-RUIZ Daniel, et al, *An Innovative and Decentralized Identity Framework Based on Blockchain Technology*, The 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), in *IEEE*, 2021, available online

OMAAR Jamila. *Forever Isn't Free: The Cost of Storage on a Blockchain Database*, on *IPDB Blog*. 2017. Available at

PATEL Nilay, *Meta's Andrew Bosworth on moving Facebook to the metaverse*, on *The Verge*, 2021, available at

PETROC Taylor. *Total data volume worldwide 2010-2025*, on *Statista*, available at the following address

PETROSYAN Ani. *Internet users in the world 2021*, on *Statista*, available at the following address

PIAZZA Manon. *The elaboration of collective representations in favor of blockchains within spaces of finance: Myth and prophecies of a possible future invested*. In *ESSACHESS Journal for Communication Studies*. 2022. Available at

QUITTEM Brandon. *Bitcoin is a Decentralized Organism (Mycelium) - Part 1 / 4*, on Medium, 2018, available at.

REED Drummond. *Does the W3C Still Believe in Tim Berners-Lee's Vision of Decentralization?* On *Evernym*, published on October 12, 2021, available at

ROACH John. *Mesh for Microsoft Teams aims to make collaboration in the 'metaverse' personal and fun*, on *Innovation Stories*. 2021. Available at

ROSS Don, *Game Theory*, *The Stanford Encyclopedia of Philosophy*, Metaphysics Research Lab, Stanford University, 2019, available at

SCHMITT Carl, trans. **KIESOW Rainer Maria**, *Law and Judgment. An inquiry into the problem of the practice of law.* EHESS. 2019.

SCHNEIDER Nathan. *Cryptoeconomics as a Limitation on Governance*, University of Colorado Boulder, 2022, available at

SCHREPPEL Thibault, *Smart contracts and the digital single market through the lens of a "law + technology" approach*, Direction générale des réseaux de communication, du contenu et des technologies, 2021.

SCHWAB Pierre-Nicolas. *RGPD Europe statistics: evolution of the number of complaints by country*, on *Marketing Tips*, 2019, available at

Secure Identity Alliance, *On the road to User-Centricity: Digital Identity in the Electronic Wallet era, An SIA guide exploring usages, policies, models and best practices*, 2022, available at

SEDLMEIR Johannes, **SMETHURST Reilly**, **RIEGER Alexander, FRIDGEN Gilbert**. *Digital Identities and Verifiable Credentials*. On Business & Information Systems Engineering. 2021. Available at

SIFFREIN-BLANC Caroline. *L'identité des personnes: une identité pour soi ou pour autrui?* Personnes et Familles - Hommage à Jacqueline Pousson-Petit, Presses de l'Université Toulouse 1 Capitole, 2016, available at.

Smart Contract Academy (collective), *Smart contracts - Case studies and legal reflections*, 2018, ecan.co.uk

Sovrin Foundation. *Self-Sovereign Identity and IoT*. 2020. Available at the following address

STALLMAN Richard. *How open source loses sight of free software ethics - GNU Project - Free Software Foundation*, available at

Statistica. *Global identity verification market size 2017-2027*, on *Statista*. Available at

SUROWIECKI James. *The wisdom of crowds*, 2005, available at

SZABO Nick. *A Formal Language for Analyzing Contracts*, on Nakamoto Institute, 2002. Available at the following address

SZABO Nick. *Formalizing and Securing Relationships on Public Networks*, on First Monday, 1997, available at

Tech London Advocates. *Blockchain: Legal & Regulatory Guidance*, on *The Law Society*, 2020.

TEMOSHOK David, **ABRUZZI Christine**. *Developing Trust Frameworks to Support Identity Federations*, on National Institute of Standards and Technology (NIST n°8149), 2018.

TREILLES Clarisse. *Conseil d'Etat validates CNIL's 100 million euro fine against Google*, on *ZDNet France*. Available at the following address

VERBIEST Thibault, **ATTIA Jonathan J**., *Internet of Universal Resources*, IOUR Foundation, 2020.

VIAL Claude, *Lexique de la Grèce ancienne, Armand Colin, 2008*, available at

Vie Publique. *Enfants sans identité : un pays sur trois concerné dans le monde*, on *Vie publique.fr*, 2020, available at the following address

Wikipedia contributors. *George Sand*, The Free Encyclopedia, available at

Wikipedia contributors. *Mosaic (web browser)*. In Wikipedia, The Free Encyclopedia, 2021, available at

Wikipedia contributors. *Public key infrastructure*. The Free Encyclopedia. 2022. Available at the following address

WOERTH Éric, Rapport d'information déposé en application de l'article 145 du Règlement en conclusion des travaux d'une *mission d'information relative aux monnaies virtuelles*, Assemblée nationale, 2019, available at.

World Economic Forum, *Bridging the Governance Gap: Interoperability for blockchain and legacy systems*, on *Centre for the Fourth Industrial Revolution (C4IR)*, 2020, available at

X. CHEN Biran and **ROOSE Kevin**. *Are Telegram and Signal the Next Misinformation Hot Spots? On The New York Times*, 2021, available at

YOUSSR Youssef, *René Carmille, un hacker sous l'Occupation*, documentary on Public Sénat, Production TSVP, 2021, available on Youtube at the following address

VI - Symposia, events and other contributions

APP and **Legal Brain Avocat**, *Build forgery-proof evidence with certified time stamping and blockchain time stamping*, Webinar, 2020.

BECKER Katrin and **KIESOW Rainer Maria**, *La promesse du droit*, seminar and talk on blockchain technologies, 27/02/2020 at EHESS, Paris.

BECKER Katrin, **LASSEGUE Jean**, **KIESOW Rainer Maria**. *Workshops on decentralized justice,* series of six four-hour workshops with a working group of researchers, EHESS, Paris.

Center de Recherches sur le Droit Public (**CRDP**). Colloquium on "*La transformation numérique du service public: Une nouvelle crise?"* January 14 and 15, 2021, available at the following address

CLUZEL-MÉTAYER Lucie, **PREBISSY-SCHNALL Catherine**, **SEE Arnaud**, **LEQUESNE-ROTH Caroline**, **HOURSON Sébastien**, et al, 2021, *La transformation du service public : une nouvelle crise ?* Ed. Mare & Martin, coll Droit & gestions publiques, 2022.

COURTIER Avocats and **AFDIT**, *AFDIT Day. Trusted third parties, blockchains: strategies and regulation - Cédric DUBUCQ - Lawyer a. BRUZZO DUBUCQ*. 2023. YouTube. Available online

ELIE Pauline, **SEGHIER Neil**, **LANGLOIS-BERTHELOT Thibault**. *Blockchain and Digital ID Wallet: towards a decentralized European identity?* Les Temps Numériques, workshop in May 2022 at EHESS, Paris, France. pp.14. Proceedings available at

FORUM DE L'AIT, Participation in the "Hackathon" ("design marathon") organized on February 7 and 8, 2023 - *Accelerating transitions for mobilities*. Available at the following address

Forum International sur la Cybersécurité (**FIC**), *Quels modèles alternatifs pour l'identité*, round table on 09/09/2021 in Lille, with Jean-Jacques Quisquater and Olivier Dussutour.

HIMMER Vincent and **PIAZZA Manon**, online seminar on *L'entrepreneuriat au prisme des sciences sociales*, February 14, 2023 from 4:30 to 6:30 pm. Presentations n°1 : *Moralizing the market. A case study of impact entrepreneurs*. Presentations n°1: *What modes of accumulation in the cryptocurrency space?* Available at the following address

INSEAD, *CEPR and INSEAD webinars on Fintech and Digital Currencies*, Webinars from September 2-15-30, 2020, available at.

Kramer Levin, *Legal Crypto webinars dedicated to fintech, blockchain and crypto-currencies*, Monday, May 18, 2020, 5:30 p.m. - 7:00 p.m.

KRYPTOSPHERE® Blockchain Summit, *A day of exchanges and meetings with the biggest players in the blockchain ecosystem*, available at

LASSEGUE Jean, **GARAPON Antoine**, *Concluding Remarks of the Seminar on Blockchain and Procedural Law: Blockchain and the Problem of Injustice*. On *Stanford Journal of Blockchain Law & Policy*. Max Planck Institute Luxembourg, 2021, available at

Paris Blockchain Society, *Decentralized identity: towards a world of sovereign users?* Round table on January 24, 2023 in Paris. With Frédéric Martin, Nicolas Caille and Thibault Langlois- Berthelot. Summary available at

PISTOR Katharina, *La loi du capital; Comment la loi crée la richesse capitaliste et les inégalités*, book presentation at EHESS, 02/05/2023

BLANC Nathalie, HAFTEL Bernard, MEKKI Mustapha et al. *Blockchain and the legal profession: the end of trusted third parties? Cycle "Between mysteries and fantasies: what future for blockchains?"*, Colloque à la Cour de cassation, 2019, replay available at.

Science Po Crypto & KRYPTOSPHERE®, *Will Bitcoin roast the planet?* Conference with Sébastien Gouspillou, Bitcoin mining specialist, April 4, 2023 from 3:30 pm to 5:00 pm, available at the following address

- A -

Digital assets: cryptographic assets designed to function as a medium of exchange, a store of value, a unit of account.

Administration: all public services responsible for managing and implementing public policies.

Amendment: proposal to modify or add information to a legal text (law, constitution, etc.).

Anonymity: the state of a person or entity that is not identifiable in a given situation.

Residual anonymity: Internet users can hide their digital identity to access certain online services.

Decentralized application: decentralized software application running on top of a quasi-decentralized protocol and generally integrating one or more smart contracts.

Sector application: see use cases.

Application-Specific Integrated Circuit: computer specially designed to run Bitcoin's mining function.

Arbitration: a dispute resolution procedure involving a neutral third party who makes an arbitration decision binding on the parties in dispute.

ASIC: specialized, machine-integrated circuit designed to efficiently perform the calculations required to validate transactions and create new blocks on the Bitcoin network.

Verifiable certificate(s): an electronic document containing information enabling its authenticity and integrity to be verified using new cryptographic mechanisms.

Identity attribute(s): any type of online or offline information designating the identity of a natural person.

Authentication: the process of verifying a user's identity using previously recorded identification information (login credentials, fingerprints, etc.).

Informational self-determination: refers to the right of individuals to control and protect their personal data.

Legal autonomy: a person's ability to determine his or her own rights and obligations, without outside influence.

- B -

Biometrics: the use of a person's unique biological characteristics, such as fingerprints, facial recognition or the iris of the eye, for identification and identity verification.

Bitcoin: the first crypto-asset born in 2009, and the origin of the first public blockchain. The latter is renowned for its reliable and resilient operation.

Bits: the smallest unit of measurement for all digital information, represented by a binary number 0 or 1 which is then interpreted by computers.

Block: group of transactions distributed in a blockchain network and registered within it.

Blockchain: decentralized digital registry of digital asset transactions held on a network of computers.

Enterprise blockchain: v. blockchain consortium.

European blockchain: reference to the 3.0 framework and infrastructures developed by the European Commission since 2018.

Closed blockchain: v. private blockchain.

Hybrid blockchain: a system that combines the characteristics of public and private blockchain, enabling flexible use for different use cases.

Open blockchain: v. public blockchain.

Private blockchain: restricted version of the public blockchain, used by a specific group of players to record and verify transactions.

Public blockchain: decentralized, transparent registry, accessible to all, where transactions a r e recorded securely and immutably.

Bluetooth: short-range wireless communication technology used to connect electronic devices such as cell phones, computers and speakers.

Regulatory toolbox: v. regulatory sandbox.

Branches of law: refers to a specific category of law, e.g. civil law, business law, etc.

Technology brick(s): reusable software or hardware module that can be integrated i n t o different systems to provide specific functionality.

- C -

Case of application: see case of use.

Use cases: situations, contexts and possibilities for the development and commercial use of a product, service or technology.

Censorship: the practice of suppressing or restricting access to information, ideas or innovations that are considered offensive, dangerous or inappropriate by a government authority, company or other organization.

Centralized: a system or organization controlled by an individual, group, company or government.

Blockchain: a distributed or decentralized database containing a list of secure transactions that can be verified more or less openly.

Value chain: all the activities of a concept, system or organization, from design to production, marketing and distribution to end-users.

Eligibility path: broad guidelines and questions that an organization can study to determine whether the use of a blockchain is necessary.

Leonine clause: abusive or unfair provision in a contract that gives excessive advantage to one party to the detriment of the other.

Private key: used to decrypt messages or transactions intended for a specific recipient

Public key: used to encrypt messages or transactions intended for a specific recipient.

QR code: digital version of data that can be scanned by a QR reader.

Source code: text written by a programmer in a programming language, which is then converted into executable code by the computer.

Unfair competition: commercial practice that consists in harming a competitor by using illegal or deceptive means to gain an advantage in the marketplace.

Competition between citizenships: competition between citizenships and identity claims specific to online communities, in relation to the concept of territorial citizenship generally adopted in society.

Terms of use: rules governing the use of a service or website, as well as the rights and obligations of users and the owner of the service or website.

Digital trust 2.0: using the technological building blocks of Web 2.0 to build trusted online systems and services.

Digital trust 3.0: using the technological building blocks of Web 3.0 to build trusted online systems and services.

Confirmation: the successful inclusion of an information transaction within a block of a blockchain.

Compliance: all the rules, standards and laws with which an organization must comply in its activities and operations.

Blockchain consensus: mechanism by which participants in a blockchain reach agreement on the current state of the blockchain and the transactions recorded on it.

Consortium: a grouping or association of companies, organizations or governments working together on a common project, while retaining their autonomy and independence.

Smart contract: a set of instructions written in code on a blockchain that executes automatically when specific conditions are met.

Ricardian contract: technological building block enabling legally formed and valid contracts to be made available or executable in digital form.

Identity checker: v. identity verifier

Corruption: abusive use of public and/or private power for personal ends, such as personal enrichment, obtaining privileges or advancing one's own cause to the detriment of the public interest.

Computer layer: level of abstraction in a computer system that enables communication between different components.

Stable crypto-assets: digital assets backed by an underlying currency or asset to maintain a stable value.

Crypto-assets: v. digital assets

Cryptographically: reference to the use of 3.0 solutions.

Crypto-currencies: v. digital assets

Cyberspace: virtual environment created by the interconnection of computer networks, such as the Internet, throughout the world.

Cybernaut: v. Internet user.

Cypherpunks: a community of Internet users who defend certain values pioneered by the Internet and new digital technologies, such as the protection of personal data, privacy and, more broadly, individual sovereignty and the right to anonymity.

- D -

DAO: decentralized autonomous organization based on smart contracts on one or more blockchains.

IT decentralization: hardware and/or software process of transferring management and responsibility for IT systems centralized by a few entities to end users and multiple business units.

Decentralized Finance: financial services based on one or more blockchains and often used without the need for an intermediary.

Decentralized identifiers: unique, permanent digital identifiers (3.0) that enable a person or organization to independently control their identity information and verify its authenticity without recourse to a centralized trusted third party (1.0 or 2.0).

Degrees of decentralization: the spectrum, i.e. the levels of IT decentralization possible for a digital system such as a blockchain.

Technological drift(s): the phenomenon whereby a technology evolves in an unforeseen or uncontrolled way due to human intervention, often leading to unforeseen applications or negative consequences.

Disintermediation: refers to a quest to reduce dependency and/or trust in one or more online third parties. Disintermediation is also mentioned in contrast to decentralization, as a lower degree (partial decentralization).

Purpose creep: see technological drift.

Developer(s): natural person who designs, creates and programs software and applications using appropriate programming languages and development tools.

Directive: a legal act of the European Union which sets objectives to be achieved by member states, while leaving them room for maneuver as regards the means of achieving them.

Digital data: data represented as binary digits, stored and processed by computers and electronic devices.

Right to identity: the right of every individual to be recognized and treated as a distinct and unique person.

Community law: the body of law applicable within the European Union, which takes precedence over the national law of member states.

Cryptographic law: v. Lex cryptographia.

Right of ownership: the right of a person to have exclusive control and disposal of a tangible or intangible asset.

Domestic law: set of legal rules in force in a specific country or territory.

Natural law: legal theory which postulates that certain laws and rights are inherent in human nature, independently of human law and culture.

Positive law: the body of law in force in a country or jurisdiction at a given time.

Digital (enhanced) rights: refers to the online exercise of certain personal rights.

- E -

Education (IT): teaching the understanding, use and programming of computers and related technologies.

Digital fingerprint: v. hash.

Online: connected to the Internet and its online services.

Epistemology: branch of philosophy that studies knowledge and scientific research.

Rule of law: the principle that the State and all institutions and persons acting on behalf of the State are subject to the law, which is applied fairly and equitably to protect the fundamental rights of citizens.

State of the art: the most recent knowledge and advances in a particular field.

State of lawlessness: characterized by the absence or collapse of the authority of the state and its legal institutions, where citizens' rights are not protected, i.e. where violence, corruption and arbitrariness are commonplace.

State-blockchain: a state's use of blockchain technologies for its administrative and public services.

Ethereum: the second-largest crypto-asset that focuses primarily on enabling blockchain-based services through the use of smart contracts, *and*

Ethereum: a partially decentralized, open source public blockchain that enables smart contracts and decentralized applications to be executed directly on its electronic registry.

Digital ethics: individual and collective morality and responsibility in the context of 2.0 and 3.0 digital technologies.

Cryptographic Euro: digital currency legally established in the euro zone and whose security and confidentiality are guaranteed by 3.0 cryptographic techniques backed by the ECB.

Digital euro: v. cryptographic euro.

- F -

Fiat: modern fiat currency like the euro and the dollar, often in electronic form rather than cryptographic.

Fungible: quality whereby two or more copies of the same thing, such as bitcoins, have identical value and are perfect substitutes for one another.

Fork: radical change to a blockchain's software protocol that invalidates previously valid blocks and transactions.

Identity provider(s): entity or organization delivering digital identity attributes.

Online service provider(s): entity or organization providing access to one or more online services.

Transaction fee: cost paid to encourage users of a blockchain to confirm a transaction on the same blockchain.

- G -

Genesis block: refers to the very first block mined on the Bitcoin blockchain.

- H -

Hashing: the act of using a computer program to transform information into a string of letters and numbers of a predetermined length.

Cryptographic hashing: mathematical function that takes variable-size data as input and generates a fixed-size digital fingerprint as output, which is unique and difficult to forge.

Halving: periodic halving of the Bitcoin issue rate, or the rate at which new Bitcoins are put into circulation by mining[1477] .

Time-stamping: the process of certifying the date, time, origin and integrity of a digital information transaction using cryptographic techniques.

Offline: digital communication without an Internet connection, thanks to other IT standards and technologies.

- I -

Decentralized identifier(s): v. decentralized identifiers.

Identification: the process of recognizing and verifying an individual's identity.

Self-sovereign (digital) identity (INAS): a set of advanced cryptographic mechanisms enabling Internet users to control and manage their own identity attributes, without recourse to any central authority to verify or validate them.

Centralized (digital) identity: a system where an individual's identification information is stored on a centralized server controlled by a central authority.

Decentralized (digital) identity: an IT solution enabling the use of decentralized identifiers, verifiable attestations and/or a blockchain to share one's digital identity in a particularly independent way (less than INAS).

Decentralized/distributed (digital) identity (IND): third-generation digital identity.

Distributed (digital) identity: IT solution enabling the use of decentralized identifiers, verifiable attestations and/or a blockchain to share one's digital identity provided by a few trusted third parties.

Third-generation identity: v. decentralized identity.

Machine identity: characteristics that make it possible to identify and distinguish the different machines in a network or computer system.

Iceberg identity: a simplified concept for breaking down identity into semantic layers, while keeping in mind its ductile aspect.

Legal identity: characteristics that help define a person or legal entity in the eyes of the law.

Genetic digital identity (4.0): digital representation of an individual's genetic information, often stored in genetic databases and used for research and identification purposes.

[1477] Visit the following website to follow these events in real time

Digital identity: personal information and traces that identify an individual to online services, including usernames, e-mail addresses, telephone numbers and credit card information.

Philosophical identity: the subjective way in which a person understands and interprets the great questions of life, such as truth, ethics, existence and knowledge.

Primary identity: attributes of a physical person's civil, legal or root identity.

Psychosocial identity: the psychological and social perception that individuals have of themselves as members of cultural groups, which influences their behavior, personality and self-esteem.

Regalian identity: v. primary identity.

Secondary identity: identity attributes that build on, complement or emancipate from a natural person's primary identity.

Social identity: personal and social characteristics that define a person as a member of a group or community, influencing his or her self-perception and relationship with others.

Universal identity: a single digital identity for every individual, regardless of nationality, religion, race or culture.

Immutable information: information that is unchanging, unchangeable and cannot be modified or altered.

Information: data and facts collected, stored and communicated online to provide knowledge and insight on specific topics.

Computer science: processing information using algorithms and computer systems.

Digital infrastructure: v. network.

Initial Coin Offering: alternative financing method based on crypto-assets, used by companies and protocols, and in which a native token is exchanged for fiat currencies or other crypto-assets.

Digital innovation: using advanced technologies and methods to create new products, services and processes that improve responsiveness, efficiency, productivity and user experience.

Public institutions: official organizations established by the State to perform specific functions and services for the common good.

Artificial intelligence: field of computer science that focuses on the creation of machines and software capable of simulating human intelligence and performing tasks that normally require human intelligence.

Internet user: a natural person who uses the Internet to access online resources and services, to communicate with other users and to carry out virtual activities.

Internet: global communications network that enables computers and other devices to connect and communicate with each other.

IT interoperability: the ability of different IT systems to exchange information and communicate with each other seamlessly and efficiently.

- J -

Lawyers: legal professionals who study, apply and interpret laws and regulations, and provide legal advice to individuals, businesses and organizations.

Alternative (digital) justice: the use of technology and digital means to provide dispute resolution solutions outside the traditional judicial system, such as online mediation and arbitration.

Decentralized justice (3.0): using blockchain technology to create dispute resolution systems that are autonomous, transparent, secure and operated by peers, without the need for a central authority. V. Kleros.

- K -

Kleros: a decentralized, blockchain-based justice platform that uses online jurors to resolve disputes quickly, transparently and fairly.

Know your business: requirements imposed by centralized service providers, often at the request of governments, who collect personal information from individuals representing corporate bodies.

Know your customer: requirements imposed by centralized service providers, often at the request of governments, who collect personal information from users and individuals.

- L -

Layer 1 & 2: protocols or platforms built (L2) alongside an existing blockchain, generally adding additional functionality or efficiency to the main network (L1).

Lex cryptographia: Latin expression meaning that cryptographic law supersedes the law of legal texts, referring to the principles and rules governing the use of computer programming, cryptography, confidentiality and data security.

Libertarian: a person who believes in the primacy of individual freedom, non-interference by the state in personal and economic affairs, and strict respect for property rights, including cryptographic rights.

Freedom of expression: a fundamental right that guarantees the freedom of all individuals to communicate their opinions, ideas and beliefs online or offline without fear of reprisal or censorship.

Lightning Network: protocol and second layer of the Bitcoin blockchain, designed for economical, fast and private payments between users.

White Paper: technical and/or commercial research document describing the purposes and/or functionalities of a crypto-asset, a blockchain or, more broadly, a 3.0 solution.

Free software: computer programs distributed under a license allowing the user to freely execute, copy, modify and distribute the software's source code.

Software: computer programs designed to perform specific tasks on computers or other electronic devices.

Natural law: moral and philosophical theory which holds that certain moral laws and principles are universally true and self-evident by reason and human nature.

- M -

Digital memory: immutable storage of the history of mankind on perennial computer media, as represented a priori by the Bitcoin public blockchain or possibly other blockchains.

Metaverse: network of 3D virtual universes focused on online immersion and social connection, often crossed with crypto-assets.

Minage: the process of computer-guessing a random number before all other participants in the Bitcoin blockchain, in order to issue new bitcoins into circulation.

Miner(s) or miners: natural or legal person in possession of an ASIC machine whose computing power is intended to extract bitcoins from this protocol for economic purposes.

Diamond business model: proposed simplified concept illustrating the main expectations of companies regarding the deployment or use of a blockchain for their business.

Cryptocurrency: v. Internet currency.

Internet currency: cryptographic currency used by Internet users for their online transactions, often independent (peer-to-peer) of traditional financial institutions.

Legal tender: currency issued and guaranteed by a State and recognized internationally as a legal means of payment in a given country.

- N -

Levels of decentralization: v. degrees of decentralization.

Node: computer involved in verifying valid transactions on the Bitcoin network.

Non Fungible Token (NFT): a cryptographically unique representation of a digital or physical asset on a blockchain.

Standardization: v. interoperability.

Standards: rules established by official bodies or industries to guarantee consistent practices and specific levels of quality or performance.

- O -

Connected object: object equipped with sensors and Internet connectivity, enabling the collection and exchange of data to improve or automate tasks.

Conventional computer: computer based on conventional information processing technology, using binary bits to store and manipulate data.

Quantum computer: a type of computer that uses the laws of quantum physics to perform incredibly fast and complex calculations.

Digital tools: see digital solutions.

- P -

Peer-to-peer: computer communication model in which each computer or node on the network can act as a client or server for the others, enabling direct sharing of files or resources without going through a centralized server.

Patrimonialization of data: the desire and process of monetizing primary and/or secondary personal data by extending property rights.

Developed countries: nations with a high standard of living, industrialized economies, advanced health and education systems, and strong, stable currencies.

Developing countries: nations with a relatively low standard of living, an undiversified economy dependent on other countries, limited access to education and infrastructure, and an unstable currency.

Peer-to-Peer (P2P): *v.* peer-to-peer.

Legal person: a legal entity, such as a company, organization or association, which has an existence distinct from its members and can act as the subject of legal rights and obligations.

Natural person: individual subject to legal rights and obligations, distinct from any company or organization.

Phygital: term used to describe an experience that combines both physical and digital elements, often used to describe interactions between the physical and virtual worlds.

Exchange platform: a platform that enables users to exchange crypto-currencies and fiat currencies.

Decentralized digital identity wallet: computer program designed to secure the private key used to access one's verifiable credentials (VC) and decentralized identifiers (DID) device specially designed to lock the private key used to access one's bitcoins

Crypto-asset wallet: device and/or program that stores the private and public keys that together allow access to the user's crypto-assets, which are stored on this medium.

Zero Knowledge Proof (ZKP): cryptographic protocol that enables a party to prove the validity of information without revealing the information itself, or any information associated with it.

Proof of existence: set of 3.0 tools enabling a person to generate and assert their physical existence online in a basic way, without this digital proof of existence representing a legally formed and legally valid identity.

Proof of legal existence: a set of 3.0 tools enabling a person to generate and assert their physical existence online in a basic way, while benefiting from legal recognition thanks to state trusted third parties.

Legal evidence: evidence admissible in court to prove or disprove a fact or allegation, which is obtained in a legal manner and presented in accordance with the applicable rules of evidence.

Programming: the process of creating a set of computer instructions that are executed by a computer or other machine to perform a specific task.

Proof-of-Authority (PoA): blockchain consensus algorithm where validators are approved entities who prove their identity and authority to validate transactions, rather than solving mathematical problems as in other consensus algorithms.

Proof-of-Stake (PoS): blockchain algorithm in which the probability that a participant will be selected to confirm a block on a blockchain is probabilistically related to the percentage of the blockchain's token supply that the participant controls.

Proof-of-Work (PoW): the algorithm on which the Bitcoin blockchain operates. Proof-of-Work is defined as the conversion of electricity into processing power.

Cryptographic property: v. Lex cryptographia.

Intellectual property: refers to the legal rights granted to creators and owners of intellectual works, such as inventions, literary and artistic works, trademarks and patents.

Protection of personal data: the process of safeguarding the privacy and rights of individuals, for example by regulating the collection, use, storage and disclosure of their personal information by third parties.

Protection of personal freedoms: preservation of individual and fundamental rights such as freedom of expression, freedom of thought, privacy, equality before the law and protection against discrimination and oppression.

Protocol: established set of rules dictating how the nodes of a blockchain interact with each other and with the code base.

Protocol (IT): a set of standardized rules, norms and procedures that enable different IT systems to communicate and exchange information in a consistent and reliable way.

Pseudo-anonymity: a privacy protection method in which an individual's identity is masked behind a pseudonym or identifier, offering relative protection against disclosure of his or her real identity, but not total protection.

Contextual pseudo-anonymity: the level of pseudo-anonymity for each Internet user needs to be adapted by design, depending on the online services they use.

Public power: all the executive, legislative and judicial powers held by the State to govern and administer a country.

- R -

Seeking anonymity: the desire and right of every Internet user to be able to surf anonymously on legal online services.

Decentralization research (IT): the will and right of every Internet user to participate in and use decentralized digital infrastructures without breaking any laws.

Legal system: the set of legal rules and principles governing a specific issue or field, such as labor law, tax law or intellectual property law.

Electronic register: v. blockchain.

(Community) regulation: a legal rule issued by the institutions of the European Union which is directly applicable to all member states without requiring national measures for its implementation.

Network (IT): a set of interconnected devices, such as computers and servers, that enable resources and information to be shared between network users.

Social networks (digital): online platforms that enable users to create profiles, connect with other users and share information, photos, videos and other content with their network of friends and contacts.

IT responsibility: the obligation to comply with laws, regulations and standards on security, data protection and privacy when using information technologies.

Legal liability: legal and/or contractual obligation to answer for acts or behavior considered illegal or harmful to a person or entity.

Identity claims: demands for recognition and respect of an individual or collective identity, which may be based on characteristics such as ethnic origin, religion, sexuality, gender or nationality.

Attribute (identity) revocation: a process that allows a user or identity provider to remove or revoke certain attributes associated with their digital identity, such as authorizations or access rights.

- S -

Regulatory sandbox: a regulated environment in which companies can test new products, services or business models without running the risk of violating existing laws.

Satoshi Nakamoto: the person or persons responsible for Bitcoin's original software code and the publication of the dedicated white paper.

Satoshis - Sats: the smallest Bitcoin unit on the chain, equal to 0.00000001 BTC.

IT security: a set of technical, organizational and legal measures designed to guarantee the confidentiality, integrity and availability of information systems.

Legal certainty: the legal principle that legal rules must be clear, accessible and predictable, to guarantee the stability of legal relations and compliance with legal rules.

Segwit: *(Segregated Witness)*, a modification of the Bitcoin protocol that increases the capacity of the blockchain while improving the security and flexibility of transactions.

Online service: service provided via the Internet, generally accessible via a Web browser, enabling users to perform various tasks, interact or obtain information.

SHA-256: cryptographic hash function used to secure transactions and information on the Bitcoin blockchain.

Sidechain: a parallel blockchain developed alongside a main blockchain. V. Layer 1 & 2

Electronic/cryptographic signature: mathematical mechanism used to prove ownership of a cryptographic key by the person holding it.

Digital society: a society in which digital technologies play a central role in social interactions, economic exchanges and cultural activities.

Solution 2.0: IT solutions using norms and standards developed in the Web 2.0 era.

Solution 3.0: IT solutions using norms and standards developed in the Web 3.0 era.

Trusted source: system, entity or person considered reliable for providing accurate information.

Digital sovereignty: an entity's ability to protect its interests in the digital world by controlling its own infrastructure and guaranteeing the confidentiality and security of its data.

Digital sphere: v. digital society.

Stablecoin: cryptographic token designed to maintain price parity with another real-world financial asset.

Staking: a blockchain-specific process in Proof of Stake (PoS) that involves sequestering one's holdings in safe crypto-assets to earn additional units in similar crypto-assets.

IT standards: norms established to guarantee the interoperability and efficiency of IT systems.

Decentralized storage: data storage method where information is distributed across different nodes in a decentralized network, rather than being stored on a centralized server.

Distributed storage: a data storage method where information is distributed across different nodes in a distributed network, rather than being stored on a centralized server.

Supranationality: characteristic of institutions and decisions that go beyond the national framework, involving concerted action by several states.

Quantum supremacy: the moment when a quantum computer succeeds in solving a problem that classical computers cannot solve in a reasonable time.

- T -

Taproot: Bitcoin upgrade designed to improve the confidentiality, security and efficiency of transactions.

Taro: Bitcoin upgrade to enable new functionalities and use cases on this public blockchain.

Hash rate: the unit of measurement of the computing and processing power of the Bitcoin blockchain.

tBDEX: decentralized exchange platform based on blockchain technology for digital assets.

Technology(ies) 2.0 : *v*. solutions 2.0.

Technology(ies) 3.0 : *v.* solutions 3.0.

Territoriality of law: the principle that legal rules are applicable only in the geographical territory in which they were enacted.

Trusted third party: an independent entity that manages and verifies electronic transactions between two parties. It may be a legal entity in the public and/or private sector that guarantees the trustworthiness of certain information and online interactions on behalf of users.

Token: unit of value on a blockchain that can integrate a variety of use cases, such as governance or a rewards program.

Transaction: entry in a blockchain that records the transfer of value or information from one user to another.

Incompatibility t r i a n g l e : concept and computer illustration specific to blockchain technology, demonstrating some of its conceptual and material limitations.

Triangle of trust: concept and illustration specific to decentralized digital identity.

- U -

Universal: something that is valid, applicable or applies, to all cases or a11 people, without exception or distinction.

Identity theft: impersonating another person by using their personal data without their consent.

Users: *v*. Internet users.

- V -

Identity verifier: person or organization responsible for verifying the identity of individuals, often as part of authentication or access control processes.

Vitalik Buterin: Russian-Canadian programmer and entrepreneur, known as the co-founder and inventor of the smart contract and blockchain platform, Ethereum.

Decentralized voting: a voting process where decisions are made by Internet users using 2.0 and/or 3.0 solutions.

- W -

Web 1.0: the first static, unidirectional version of the World Wide Web, where users could only view Web pages but could not contribute to their content.

Web 2.0: evolution of Web 1.0, characterized by interactive websites and social networks that enable users to actively participate in online content creation.

Web 3.0: a new version of the Internet based on blockchain technologies and decentralized identity.

Dictionary of acronyms

- A -

European Banking Authority *(EBA)*
ABFalliance blockchain France
ACPRautorité de contrôle prudentiel et de résolution (Prudential Control and Resolution Authority)
ADANassociation for the development of digital assets
DNAdeoxyribonucleic acid
AECautomated clause enforcement *(smart contract)*
AEFRassociation europe finances regulations
ESMAEuropean Securities and Markets Authority
AEPDagencia española de protección de datos
AESadvanced encryption standard
AFADPPassociation francophone des autorités de protection des données personnelles AFDIannuaire français de droit international
AFNORassociation française de normalisation
AGRASorgane de gestion et de recouvrement des avoirs saisis et confisqués ALICEMauthentification en ligne certifiée sur mobile
AMFauthorité des marchés financiers
ANSSIagence nationale de la sécurité des systèmes d'informations (French national agency for information systems security)
AP-HPassistance publique hôpitaux de Paris
APIapplication *programming interface*
ARaugmented reality *(augmented reality)*
ARCEPAuthorité de régulation des communications électroniques, des postes et de la distribution de la presse (French regulatory authority for electronic communications, post and press distribution)
ARPANETadvanced research projects agency network Art. article
ASICapplication specific integrated circuit

- B -

B2G business-to-government
BaaSblockchain as a service
BaFin bundesanstalt für finanzdienstleistungsaufsicht *(federal authority created in 2002)*
BAHTXBaidu, Alibaba, Huawei, Tencent, Xiaomi *(the 5 Chinese Web giants)*
BCChinese Central Bank
ECBEuropean Central Bank
BCGboston consulting group
BCIDblockchain and digital identity
BCNblockchain notarial
BFDIder bundesbeauftragte für den datenschutz und die informationsfreiheit BICbusiness indentifier code
BIPbitcoin improvement proposal
BISbank for international settlement *(BRI in French)*
BMCbitcoin mining council
Bank for International Settlements *(BIS an aglais)*
BTCblockchain bitcoin
BtoB business-to-business

BtoC	business-to-consumer *(data sharing between companies and consumers)*

- C -

CAcour d'appel
CASPcrypto-asset service provider *(PSAN)*
Cass. cassation
CBDCcentral bank digital currencies *(MNBC)*
Pan-Canadian confidence framework
CCPAcalifornia consumer privacy act *(United States)*
CCPAcalifornia consumer privacy act *(United States)*
CCTstandard contractual clause
CDHuman Rights Council
CEuropean Commission
ECHReuropean Convention on Human Rights
European Data Protection Committee *(EDPB)*
CERNEuropean Organization for Nuclear Research
cf. confer *(Latin)*
CICEcrédit d'impôts pour la compétitivité et l'emploi (tax credit for competitiveness and employment)
ICRConvention on the Rights of the Child
CIRresearch tax credit
Civ. civil
CJEUcourt of Justice of the European Union
CMFmonetary and Financial Code
CNCJNational Chamber of Judicial Commissioners
National identity card
CNIdigital national identity card
CNILcommission nationale de l'informatique et des libertés
CNNumconseil national du numérique
CNRScentre national de la recherche scientifique
UNCITRAL United States Commission on International Trade Law
UNCITRALUnited Nations Commission on International Trade Development
Cold Wallet cold storage wallet*(offline generation and storage of keys)* CSDHLF Convention for the Protection of Human Rights and Fundamental Freedoms CSPcatégories sociaux professionnelles
CtoB consumer-to-business *(data sharing between consumers and businesses)*

- D -

DADDUEprovisions for adapting to EU law *(law no. 2023-171 of 9.03.2023 transposing Directive 2019/882 of 17.04.2019 into French law)*
DAMdigital asset *management (GAN)*
DAOdecentralized autonomous *o r g a n i z a t i o n (OAD)*
DAppsapplications décentralisées de nouvellesgenerations DataAct (Regulation) European data regulation
DCPersonal data
DDHConstitution of Human and Civil Rights
DEEPdistributed *ledger technology (DLT)*
DeFidecentralized finance
DeSocdecentralised society
DGA (Regulation) data governance act *(European Data Regulation)*
DGEdirection générale des entreprises

DIDdecentralized identity

DID4ALLdecentralized identifiers for all

DIFdecentralized identity foundation

DINUMInterministerial Digital Department

dir. under the direction of

DLCdistrict log contract

DLTdistributed ledger technology *(DEEP)*

DMAdigital markets act

DNIedocumento nacional de identidad electronica *(Spain)*

DPKIdecentralized public key infrastructure

Data protection *officer* (DPO)

DSAdigital services act *(United States)*

UDHRuniversal Declaration of Human Rights

- E -

EBAeuropean banking *authority*

EBSIeuropean blockchain service infrastructure

e-CNYe-digital Chinese yuan *(or digital renminbi)*

Ed. edition

EDIelectronic date interchange *(electronic data interchange)*

EDICeuropean digital infrastructure consortium

EDIWeuropean digital *identity wallets*

EDPBeuropean data protection board *(CEPD in French: conseil européen de la protection des données)*

EDRIeuropean digital rights

EEAentreprise euthereum alliance

EEAuropean Economic Area

EHESSécole des hautes études en sciences sociales

eIDelectronic digital identification

eIDAS 1 (Regulation) electronic identification authentication and trust *services*

eIDAS 2 (Regulation*)* electronic identification authentication and trust services

EMEetablissement de monnaie électronique

ENISAeuropean union agency for cybersecurity

ESMAEuropean securities and markets authority *(AEMF in French)*

ESSIFeuropean self-sovereign identity framework

etc. etcetera

ETH euthereum

ETSIeuropean telecommunication standard institute

EUROCeuro coin

- F -

FATFfinancial authority tasks force *(GAFI in French)*

Key success factors

FEDfederal reserve system

FICforum international cybersecurity forum

FINMAswiss financial market supervisory authority

IMFInternational Monetary Fund

FNTConfédération des tiers de confiance du numérique (Federation of trusted digital third parties)

- G -

G20group of twenty
GAFAMGoogle , Apple, Facebook, Amazon, Microsoft
FATF Financial Action Task Force *(FATF)*
Digital asset management (DAM)

- H -

OHCHR Office of the United Nations High Commissioner for Human Rights
UNHCRUnited Nations High Commissioner for Refugees

- I -

AIartificial intelligence
IAMidentity and access management
IBANinternational bank account number
Ibid. ibidem *(from Latin, meaning from the same author, same work as the previous reference)*
ICOinitial coin *offering*
Id. idem
IoTInternet of things
IDPidentity provider
IEOinitial exchange offering
In in
INASelf-sovereign digital identity
INDecentralized/distributed digital identity
Below *(Latin*)
IONidentity overlay network
IoTinternet of things *(IdO)*
IPinternet protocol
IPFSinternet protocol files system
ISOInternational Organization for Standardization *(founded in Geneva in 1949)*
ISPinternational organisation for standardisation
ITVinternational communication union

- J -

JNF non-fungible token
JOEAgistered electronic official journal
JORFjournal officiel de la république française
OJEUofficial Journal of the European Union

- K -

KPIkey performance indicatror
KYBknow your business
KYCknow your costumer

- L -

L1layer 1
L2layer 2
LBCAlegal blockchain and crypto association.

LCB-FTlutte contre le blanchiment et le financement du terrorisme LGDJlibrairie générale de droit et de jurisprudence
LLMliberland sea
LNlightning network
LoAlevel of assurance
LIL loi informatique et libertés *(n° 78-17 of January 6, 1978)*
LOPPSI (law) loid'orientation et de programmation pour la performance de la sécurité intérieure *(*orientation and programming lawfor the performance of internal security*) (n° 2011-267 of March 14, 2011)*
LSCliberland smart chain

- M -

MC&Mmobile connect & moi
MiCA (law) marketsin crypto-assets *(crypto-asset markets, law no. 2020/0265 of September 24, 2020)*
MiFID 2market in financial instrument directive
MNBCentral bank digital currency *(CBDC)*
MRmixt reality

- N -

NFCnear-field communication *(Spain)*
NFTnon fungible token

- O -

ICAOInternational Civil Aviation Organization
SDGsustainable development goals
ODRonline dispute *resolution*
OFACoffice of foreign assets control
WIPOWorld Intellectual Property Organization
ONUorganisation des nations unies
Op. cit. opus citatum *(work cited, Latin)*
OPOCEoffice for Official Publications of the European Communities

- P -

p. page(s)
P2Ppeer to peer
P2Ppeer to *peer*
PACTE (law) action plan for business growth and transformation *(law n°2019- 486 of May 22, 2019)*
PBoCpublic bank of china *(banque populaire de chine)*
PCBpre-commercial procurement
PDFportable document format *(PDF document)*
PEDdeveloping countries
PFIparticipating financial institution
ICCPRInternational Covenant on Civil and Political Rights
PINDecentralized digital identity portfolio
PIPLpersonnal information protection law
PKIpublic key infrastructure
PNKpinakion *(digital utility token)*
PoAproof of authority
PoHproof of humanity
PoSproof of stake

PoWproof of work
Digital Asset Service Provider *(CASP)*
PSCA-crypto asset service provider *(CASP)*
PUFpresse universitaire de France
PVIDemote identity verification provider

- Q -

QR codequick response code

- R -

RCSregistre du commerce et des sociétés
REFrevue d'économie financière
RGPDrèglement général sur la protection des données à caractère personnel (General regulation on the protection of personal data) RNIPPrépertoire national d'identification des personnes physiques (National directory for the identification of natural persons)

- S -

s. d. no date
SaaSsoftware as a service
SAMLsecurity assertion markup language
SBTsoul bound token
SCICsociété coopérative d'intérêt collectif (cooperative collective interest company)
SDNsociety of Nations
SECsecurities and exchange commission *(United States)*
SGINservice de garantie de l'identité numérique (digital identity guarantee service)
SIMsubscriber identity module
ISMSinformation security management system
SSI *self-sovereign identity*
SSOsingle sign on
STOsecurity token
supra above *(Latin)*
SWIFTsociety for worldwide interbank financial telecommunication

- T -

TCPtransmission control protocol
TCRtoken curated registries
TEStitres électroniques sécurisés
TFRtransfer of fund regulation
TFEUTreaty on the Functioning of the EU
Th. thesis
TRACFINtraitement du renseignement et action contre les circuits financiers clandestins TROtemporary *restrictive* order

- U -

UBIuniversal basic income *(token)*
EU European Union
UETAuniform electronic transactions act *(United States)*
International Telecommunication Union
UNHCRUnited Nations Refugee Agency
UNICEFunited nations international children's emergency *fund*
URLuniform resource locator

USDCUSD coin

- V -

V. *VCverified credentials* see

VPverifiable presentation
VRvirtual *reality*

- W -

W3Cworld wide web consortium
Walletportfolio for crypto-currencies
WEFworld economic forum
WiPOworld international property office

- Y -

YCCeYuan digital

- Z -

ZKPzero knowledge proof

Appendices

Appendix 1: Twenty-one questions for understanding identity in the 21st century

1	*Why define identity?*
2	*Do we need to define identity?*
3	*What is identity?*
4	*What is digital identity?*
5	*How do you define legal identity?*
6	*How do we define social identity?*
7	*How to define philosophical identity?*
8	*How to segment digital identity?*
9	*Is identity a social, legal or digital fact?*
10	*Is a universal identity possible?*
11	*Is a universal identity desirable?*
12	*What's the difference between the right to an identity and the right to a universal identity?*
13	*Technological developments in identity?*
14	*Are new technologies at the service of identity?*
15	*Is data who we are and who we are not?*
16	*Is blockchain technology helping to liberate people's digital identity?*
17	*What is decentralized digital identity?*
18	*Is decentralized identity the future of digital identity on the Internet?*
19	*Why is financial identity so important in the digital age?*
20	*What are the legal and social impacts of decentralized identity?*
21	*Will the future of identity be genetic?*

Appendix 2: Summary table of issues and hypotheses by level of abstraction

Level of abstraction (A - C)	Issues addressed	Assumptions
Level A *(Structural issues)*	• Do 3.0 technologies impact people's legal and primary identities? Their secondary identity?	• Yes. Yes.
	• Is blockchain a revolution for digital identity? For society?	• Yes. Yes.
	• Will Metavers have an impact on Internet users' digital identity?	• Yes.
	• Should blockchain technology be distinguished from Bitcoin?	• No, except for digital identity.
	• Would decentralizing the entire company be beneficial?	• No.
	• Would decentralizing the entire Internet be beneficial?	• Yes
	• Is decentralized digital identity a revolution that complements and follows on from digital identity 2.0?	• Yes
	• Do blockchain and IND have technological variants?	• Yes
	• Is there an inseparable link between digital identity 3.0 and crypto-assets? Between the Web 3.0 and crypto-assets?	• Yes. Yes.
	• Do blockchains, crytoactives and IND converge in terms of the history of computer science to meet the need for new digital counterpowers?	• Yes.
Level B *(Related issues)*	• Does blockchain threaten state sovereignty and monetary monopoly?	• Yes and no.
	• Does the IND threaten sovereignty and the monopoly of identity?	• Yes and no.
	• Does the decentralization of IT serve Internet users' online rights and freedoms?	• Yes and no.
	• Is a new cryptographic law necessary and feasible?	• Yes

	• Should online cryptographic property rights be recognized? • Is a right to online pseudo-anonymity necessary? Is anonymity also necessary? • Should the law take hold of new cryptographic methods that, by design, respect Internet users' data? • Do public blockchains suffer from a lack of legal compliance? • Does the IND strengthen the exercise of people's rights online? • Does part of the success of 3.0 technologies lie in their resilience and global IT interoperability? • Can decentralized justice replace traditional justice? Can it make it more transparent and efficient?	• Yes and no. • Yes. Yes. • Yes. • No and yes. • Yes. • Yes. • No. Yes.
Level C *(Subsidiary questions)*	• Will official identity documents disappear? Will they all be dematerialized? • Is a universal digital identity desirable? Viable? • Should Bitcoin and its computer consensus mechanism be restricted or banned? ? • Can public authorities build 3.0 trust infrastructures for the digital identity of their citizens? Should it finance them? • Can blockchain and IND provide reliable digital proof of existence as a basis for legal identity? • Could quantum supremacy revolutionize Web 1.0, 2.0 and 3.0? • Is a digital and genetic identity possible?	• No. Yes. • Yes. No. • No. • Yes. No. • Yes. • Yes and no. • Yes.

Appendix 3: Focus on Bitcoin

Focus 1: What is Bitcoin?

Today, the accepted practice of the Bitcoin community is to use the term Bitcoin (singular with capital **B**) to designate this computer network, protocol and/or community. The term bitcoin (with a lower-case **b**) refers to the cryptographic units or tokens with monetary value (whose acronym is "BTC") that circulate on this IT infrastructure. These cryptographic units of account enable near-instantaneous payments to be made to anyone, anywhere in the world, via a simple Internet connection (sometimes without one). Openly accessible to Internet users since 2009, Bitcoin uses a suite of complementary technologies to operate without central authority(ies) and in a highly decentralized way, and in particular inspired by over 40 years of research and development in computing technologies[1478] . Transaction management and the issuance of its native crypto-asset (bitcoin - BTC) are carried out collectively by a network of computers called "nodes"[1479] . These machines are (pseudo)anonymous and geographically distributed throughout the world. Rather than relying on central authorities to operate, the Bitcoin protocol relies on mathematical and cryptographic mechanisms to control the creation and transfer of tokens. Over the past decade or so, Bitcoins have gradually come to be regarded by some Internet users as the Internet's currency, whose scarcity has been mathematically verifiable and gradually demonstrated since its inception. Given the history and positioning of this experimental currency for some, or quasi-currency for others, bitcoin today represents a benchmark for the market in blockchain technologies and the crypto-assets that it has spawned. Its design and code have inspired the majority of crypto-assets that are trying to emancipate themselves from the computing world, but it is clear that bitcoin remains the first and foremost permanent financial application of an open blockchain. In a way, this IT infrastructure represents an alternative, dematerialized and decentralized monetary and community system. Its community generally refers to interactions between machines ("nodes" and "miners")[1480] , developers and users/investors. In other words, its main characteristics can be summarized as follows:

[1478] HELD Dan, "Planting bitcoin - soil (3/4)", in *danheld.com*, 2018, available online.
[1479] For just a few hundred euros, you can set up your own *bitcoin node, i*.e. a physical and digital management and storage system for your bitcoins, right in your own home. In this way, Internet users can manage their own 3.0 online bank. See below.
[1480] V. Appendix 6, Focus 1.

Summary of Bitcoin's main features
Simple mobile and web payments (via QR codes, links, etc.)
(Mathematical) security and (cryptographic) control of tokens by users
Since 2009, bitcoins can be transferred over the Internet and sometimes without it (SMS[1481] or radio).[1482]
Fast or instant international payments
Low (main network) or zero (Lightning Network) costs
Preservation of user identity by design (pseudo-anonymity)

What's it for?

It simply enables value to be sent and received as a "peer-to-peer electronic cash system"[1483] , without geographical discrimination, using a computer, telephone or simple Internet connection. In the not-too-distant future, Bitcoin may be able to accommodate new use cases (NFT[1484] , stablecoins, P2P social networks) thanks to adjacent protocols currently under development, as detailed below.

Why is it revolutionary?

Since Bitcoin is both a cryptocurrency and an aggregate of open computer protocols on the Internet, a relatively objective understanding of its IT, economic, social and legal aspects requires several years of continuous learning and observation. Unlike other methods of transferring values and currencies over the Internet, bitcoin exchanges operate in principle without the need to trust an intermediary[1485] . The very fact that this system can function and be used without a trusted third party means that it represents the first public and cryptographic payments infrastructure - distributed or decentralized - in the world.

[1481] HALL Joe, "Bitcoin without Internet: SMS service allows sending BTC with a text", in *Cointelegraph*, 2022, available at.
[1482] Ledger, "School of Block Episode 4 - Bitcoin by Radio, This can't be possible!", in *ledger.com*, 2022, available at.
[1483] NAKAMOTO Satoshi, "Bitcoin: a Peer-to-Peer electronic cash system", available online at
[1484] See, for example, the "*Ordinals*" protocol in Focus 3 below.
[1485] *Op. cit.* In fact, according to a March 24, 2023 study, 80% of holders of crypto-assets (including bitcoin) host and store them within a platform and a trusted third party, and only 30% hold them cryptographically on one or more unhosted wallets. For more information, please see the following information, Coingecko,
"Where People Store Their Crypto, Post-FTX Collapse", March 24, 2023, available at.

world. This open network is accessible to all, and does not belong to one or more players who could take significant control of it. Before Bitcoin, there were only a few public infrastructures enabling the free exchange of information, such as the Internet, which remains - with difficulty to this day[1486] - the most important open infrastructure in terms of size and stakes. In the monetary sector, the main public payment infrastructure accessible to all is fiat money (paper bills and metal coins), which today only functions for face-to-face transactions, which is a form of limitation compared to Bitcoin, whose vocation is relatively similar (possibility of pseudo-anonymity and exclusive ownership when making payments), but whose exclusively digital nature and form reinforce its relevance in terms of use and reach in the digital age. In other words, before Bitcoin, if one person wanted to pay another remotely using a phone or computer, it was complicated, if not impossible, to use a public digital infrastructure, and ultimately necessary to turn to private players (banks, mobile companies, large technology firms), i.e. to trust their accounting and financial systems and records. In concrete terms, this means that Internet users have to use multiple online services, subjecting themselves de facto to recurring validation of their transaction requests with these third parties (IT dependency), whom they also have to trust over a long period of time (social dependency). With the Bitcoin blockchain[1487] , anyone can now add a transaction to this public register by transferring fractions of bitcoins to other users. A bitcoin can be split up to eight decimal places, making it possible, for example, to send the equivalent of a few euro cents in bitcoins to its users[1488] . This means that, for the first time, any Internet user, regardless of border, creditworthiness, nationality, gender or religion, can access a bitcoin address free of charge to receive or transmit bitcoins via this public infrastructure. As a result, Bitcoin symbolizes and represents a form of computerized and individual freedom in its purest form. It is computer-immutable, as its blockchain is theoretically impossible to corrupt, i.e. to hack, unlike its social ecosystem of applications, which remains fallible, as Appendix 7 underlines. This quasi-monetary and open financial network is socially resilient thanks to the thousands of individuals who record and store each of its transaction blocks on their personal computers (nodes)[1489] , which means that they

[1486] Gouvernement, "Câbles sous-marins de communication", in *L'économie bleue en France*, Ed. 2022, "The rise of the Internet and financial globalization has considerably increased the dependence of States on submarine communication cables. It has been estimated that $10,000 billion worth of financial transactions pass through submarine communication cables every day. A cable malfunction can have major consequences for a state. [...] New issues such as the emergence of large private groups - essentially the GAFAMs - in the global cable business and the risks of a potential challenge to the principle of net neutrality must also be particularly closely monitored", p. 4, consulted on 08/01/2023 at the following address

[1487] V. Appendix 6, Focus 1.

[1488] By way of illustration, since 2021, the social network Twitter has offered a new feature for making donations in bitcoins between users. This means that any Internet user can, in theory, receive funds almost free of charge, provided they have Internet access (opening a Twitter account is free). See an example of a dedicated Tweet.

[1489] Take a look at the next page to see the estimated number of *nodes* distributed around the world in real time. For just a few hundred euros in total, you can set up your own *bitcoin node, i*.e. a system for managing and controlling your bitcoin.

can provide the community with the complete history of these blocks - automatically saved on their computers - should the need arise (community update, hacking, bug).

Can it be considered a currency?

In 2009, the launch of bitcoin was partly motivated by the need to avoid the abuses of the financial sector that led to the 2008 financial crisis[1490] . Although it was not directly widely recognized as a viable global electronic cash system at the time, its growing popularity and confidence meant that by 2023 it was approaching Aristotle's famous definition of a currency. According to him, a currency must fulfill three key, cumulative functions: it must be a unit of account, a means of exchange and a store of value. By balancing exchanges, it therefore facilitates trade and develops social relations[1491] . At present, bitcoin appears to fulfill the first two key functions of a currency, and is likely to fulfill the third in the future[1492] . Furthermore, the definition of money in the sense of the French philosopher Joseph Moreau[1493] seems to correspond to the fact that bitcoin could become a currency in its own right, as is already the case in El Salvador (see Appendix 5), provided it achieves a sufficiently large social and political consensus in the future. In short, bitcoin has made significant progress since its creation in 2009, and continues to evolve towards a more complete definition of currency. However, bitcoin's ultimate status as a legal tender depends *ultimately* on majority social and political acceptance, which may be possible in the long term, albeit utopian, given the current state of the texts that are progressively framing its ecosystem[1494] . In March 2023, however, bitcoin can already be considered the currency of the Internet, as more than one billion bitcoin addresses have already been involved in a transaction[1495] , and more than 300,000 transactions are carried out every day on this network[1496] . It can thus be asserted that bitcoin is used daily by a relatively large number of individuals, particularly in developing countries.

---

storage of bitcoins, directly at home. In this way, every Internet user becomes his or her own bank. For more information, see the solutions and computer peripherals (*nodes*) offered by *Umbrel* and *Nodl.*

[1490] NAKAMOTO Satoshi, "The problem with this solution is that the fate of the entire monetary system depends on the company that manages the minting of money, with every transaction having to go through it, like a bank", 2008, available online at p.2.

[1491] Aristotle theorizes the principle of balanced exchange and the three main functions of money, 2022, in *citeco.fr*. Available online, "Money serves as a unit of account, an intermediary in exchanges and a store of value. By balancing exchanges, it facilitates them, enabling everyone to better satisfy their needs and developing social relations".

[1492] In 2029, bitcoin will have been around for 20 years, which will probably give us a better idea of the extent to which it has fulfilled its function as a store of value.

[1493] MOREAU Joseph, " Aristote et la monnaie ", in *Revue des Études Grecques*, tome 82, fascicule 391-393, 1969, pp. 349-364, " La monnaie est alors une institution, non seulement en ce sens qu'elle a été instituée, établie par une convention [...], mais parce qu'elle est devenue un usage courant (currency), qui s'impose en vertu de la coutume, des idées reçues, à peu peu comme l'usage de la langue. The very name that designates it [...] indicates that it does not derive its value from nature, but from common opinion, from the law", available at the following address

[1494] V. Appendices 7 and 14

[1495] For more information, consult this number in real time at Glassnode Studio, "On-Chain Market Intelligence". However, users may have more than one bitcoin wallet address or keep their bitcoins on centralized exchange platforms (trusted third parties), making it difficult to estimate the exact number of people using bitcoin worldwide.

[1496] For more information, consult this number in real time at the following address, in *BitInfoCharts*.

Is it perfect?

If Bitcoin initially seemed to align itself with the "*technological solutionism*" trend[1497] , it seems that the "Web 3.0" movement is more in line with it. This is a common misconception, however, as Bitcoin is certainly part of the Web 3.0 movement, but with a very specific positioning that implies that it does not claim to be the ultimate technological solution to all the digital ills mentioned in this research. Indeed, because the promises of Web 3.0 are not yet concrete (Defi, NFT), Bitcoin has been proving its worth for over 14 years in the IT and social spheres, but almost exclusively in the monetary and perhaps soon financial realms (*see* Focus 4 below). Nevertheless, as a distributed cryptocurrency, and therefore supposedly independent, its price is not as stable as an official, government-issued currency, and it serves mainly as an alternative form of payment or as a store of value (its cryptographic rarity earning it the apt appellation of "digital gold")[1498] . Although on the one hand it has gained notoriety as a safe-haven asset among a growing community of Internet users, it is not yet widely accepted as a means of payment worldwide in comparison with legally regulated currencies[1499] . There is probably still a long way to go before bitcoin becomes a universal monetary solution. In the meantime, it is clear that bitcoin represents an unprecedented new asset in the world of payments and, more broadly, in digital finance. It is therefore likely that the monetary revolution initiated by bitcoin is still in its infancy. In some cases, existing private payment systems may be enhanced or even replaced by this public payment network 3.0, underpinning the likelihood that other private digital systems will gradually turn to this trusted public infrastructure, yet without any significant trusted third parties likely to censor this network. In a few years' time, Bitcoin may no longer be limited to the monetary domain, but could also be used for other purposes and contexts, such as the management of digital identities (IND/INAS), accounting records, social networking platforms or even video games (metavers). While the Bitcoin protocol and other similar systems are not yet mature enough to meet certain societal, IT, political and economic challenges, they have since their launch represented a serious alternative and a hope for at least partial solutions in the future. It is therefore important for the EU to promote and implement more accommodating policies to encourage the emergence of alternative public IT systems that will benefit the common good, European legal certainty and the financial and digital freedom of European citizens.

[1497] MOROZOV Evgeny, "To solve everything, click here: the aberration of technological solutionism", 2014, Ed. Fyp. Technological solutionism refers to the belief that all social and political problems can be solved by technology.
[1498] V. Appendix 6, Focus 1.
[1499] The following interactive map shows over 8,000 businesses that will be accepting bitcoin as a means of payment in 2023.

Should it be banned?

Because the notion of IT, social and economic decentralization is just a specter, as this research shows, this difficult 'confiscability' of bitcoins fundamentally disturbs the established order. However, this global decentralization seems limited in the long term, due to a gradual social and economic recentralization of bitcoins, which the protocol's IT decentralization alone probably cannot prevent (it must also be accompanied by a willingness and quest for global decentralization by Internet users of their bitcoin holdings). For all that, it seems complex and ineffective to ban Bitcoin, although it is essential to put in place regulations and laws to frame its uses and ensure the legal security of users and companies involved in this promising infrastructure for an Internet 3.0. Many countries have already adopted specific rules to govern the buying and selling of[1500] crypto-assets (bitcoin included), trying to take into account each of the IT characteristics and purposes of these assets, which are in reality mostly IT-centralized (the antithesis of Bitcoin's quest for continuous decentralization). These rules may include compliance and transparency requirements for the companies that use or offer these assets, or accounting and tax reporting obligations for the individuals who own and use them. By establishing appropriate but proportionate regulations, it would be possible to protect consumers from illegal activities that have effectively been facilitated by bitcoin in the past[1501] . However, depending on the technical stakeholders of a blockchain technology, such as its users, investors, node operators as well as French and foreign companies operating in its ecosystem, regulation is often perceived as an attempt to interfere, i.e. centralize and control, over this nevertheless decentralized computing protocol (*see* Appendix 7). In response to these regulatory demands, some of which are out of proportion, and whose political motivations no longer seem to be hidden as has been demonstrated, a social movement driven by "*decentralization maximalist*" individuals[1502] and in favor of protecting the Bitcoin protocol, is making itself heard on the Internet. At the time of writing, it is unlikely that a partial or total ban on Bitcoin will lead to its disappearance, as some researchers are suggesting[1503] . In fact, the network has been in existence for over 14 years by virtue of the aforementioned "Lindy effect", and has yet to come under computer attack from a consortium of states or corporations. Attacks are more likely to be politically motivated, as this research reminds us. Instead of

[1500] V. Appendix 14

[1501] After its launch, Bitcoin was rapidly adopted as a form of digital currency on illegal online platforms, both visible and hidden on the Internet. Although the majority of Bitcoin transactions are now legal, this tumultuous history has left a stigma that continues to cause confusion between these legal and illegal uses of this digital currency. This study also shows that this past image has become a political argument rather than a pragmatic one.

[1502] See *above*, I, Title 2, 2.1.3

[1503] DUFRENE Nicolas, DELAHAYE Jean-Paul, et al, "Il est urgent d'agir face au développement du marché des cryptoactifs et de séparer le bon grain de l'ivraie", Tribune de l'Institut Rousseau, February 8, 2022, accessed October 18, 2022 at.

to ban it[1504] , it would seem preferable to deal with this innovative computer protocol, and even to encourage its various uses, particularly in view of its social and digital benefits (*see* Focus 3 to 6). So, rather than seeing Bitcoin as a societal threat requiring a direct or (more likely) indirect legal ban, it seems wiser to approach it as an opportunity for businesses and organizations that can already explore new forms of digital transactions that are more verifiable, resilient and secure.

Focus 2: The Bitcoin protocol's IT resilience in the face of a fragile ecosystem For the Bitcoin blockchain to guarantee its operation and IT security, it needs to attract new users, on the one hand to achieve a network effect sufficient to ensure its decentralization and IT resilience, and on the other to affirm its social utility in terms of

energy, as discussed in the following Appendix. Among these users and investors, some become network validators ("miners") in return for automatic and variable remuneration in bitcoins for their material and electrical contribution to securing this protocol. In this respect, the creation of bitcoins must follow strict issuance rules[1505] , such as a limited quantity as well as restricted issuance of new tokens, rules commonly defined and modified by its community of Internet users (developers, miners). This transparent, readable and accessible operation enables Bitcoin - in the eyes of its growing number of users - to be endowed with a progressively increasing use and reserve value, as a result of the supply and demand for Bitcoins on the Internet. To take this process a step further, a user - nowadays often a professional - extracts bitcoins by running a software program that seeks the solution to a mathematical problem that takes a long time to solve[1506] and whose degree of difficulty is precisely known. This degree of difficulty (*see* Appendix 6, Focus 1) is then automatically adjusted according to a computer-predictable schedule, so that the number of solutions found for a given unit of time is constant. In this way, the Bitcoin network targets around six solutions per hour, or one every ten minutes[1507] . When a solution is found, the user's machine

---

[1504] To see in real time which countries have banned or authorized Bitcoin, consult the following interactive map, in *Bitrawr,* "Bitcoin Legality by Country Map".

[1505] NAKAMOTO Satoshi, "The nature of Bitcoin is such that, as soon as version 0.1 was released, the fundamental design was fixed for the rest of its lifespan. That's why I wanted to design it to support every possible type of transaction I could think of. [...] If Bitcoin is very successful, these are things we'll want to explore in the future, but they all had to be designed from the start to make sure they would be possible later on. I don't think a second compatible implementation of Bitcoin will ever be a good idea," in
"Transactions and Scripts, June 17, 2010, available online at

[1506] In reality, miners don't directly produce bitcoins, they produce blocks. If they are valid, miners are automatically rewarded with bitcoins by the protocol. As the bitcoin issuance schedule is fixed and stable over time, more energy used for mining does not mean more bitcoins will be mined. Therefore, what many today call "*mining"* will continue after the last bitcoin has been *mined. Consequently,* the term "*mining*" or "*extraction*" is semantically misleading and inappropriate, and could be referred to as "*block production*". However, for the sake of intelligibility, it is commonly accepted in the Bitcoin ecosystem to retain the term "*minage"*, preferred here.

[1507] NAKAMOTO Satoshi, "This is a globally distributed database, with additions to the database consented to by the majority, according to a set of rules they follow: - Every time someone finds proof of work to generate a block, that block receives new coins [bitcoins]. - The difficulty of

automatically informs the rest of the network of the existence of this newly-found solution, along with other information grouped together in what is known as a "block (of transactions)". Note that while each solution is deliberately time-consuming for "miners" (validating computers) to find, they are easy to verify by the other nodes in the network (less specific and powerful verifying computers), since the path to this solution has already been traced by a validator and then very quickly propagated, verified and approved by the other verifying nodes in the network, which store the history of said blocks.

The computer validation process and mechanism mentioned above, which currently consumes a significant amount of electricity, is known as Proof of Work (PoW), as detailed at the beginning of Appendix 6. Thanks to this mechanism, any block created by a malicious user that does not respect the protocol's common rules will be rejected by the other network participants (miners and/or nodes). In concrete terms, for each bitcoin transaction, each piece of information is sent and transmitted to as many computers and nodes on the network as possible. In this way, a register is created in the form of an ever-growing chain of blocks, collectively maintained by a very large number of machines and computers (each of which possesses a complete copy, thus preventing any loss of data and ensuring optimal, lasting resilience of the cryptographic chain's transactions). In fact, all the blocks are automatically linked cryptographically in such a way that, if one of them were to be modified, all the preceding and following blocks would have to be recalculated, which is computerically impossible given the current state of computing knowledge.

However, while Bitcoin is theoretically immune to computer attacks, as demonstrated by the fact that it has been operating without a major incident for over a decade[1508] , its ecosystem is not, as evidenced by the recurrent and multiple cases of scams, thefts[1509] or the freezing, seizure and confiscation by legal means of ill-gotten bitcoins. This is due to the significant IT decentralization that protects its protocol, rather than its ecosystem of players, which remains mostly centralized in IT and social terms, as illustrated in Appendix 7. We can also point to several sources of dependence on Bitcoin, notably the

proof of work is adjusted every two weeks to aim for an average of 6 blocks per hour (for the whole network). - The number of pieces given per block is halved every 4 years. You could say that coins are issued by the majority. They are issued in limited and predetermined quantities", February 18, 2009, available online at [1508]. Reference is made to a case of hacking that occurred on the Bitcoin blockchain in August 2010. Contrary to popular belief, Bitcoin has in fact already been successfully hacked: a hacker exploited a flaw in its code to generate 184 billion bitcoins (whereas the total number of bitcoins in circulation is limited to 21 million bitcoins, as discussed below). The bug was corrected within a few hours by Satoshi Nakamoto himself. The person behind this event, known as "The value overflow incident", remains unknown to this day. V. "Strange block 74638", in *bitcointalk.org* on August 15, 2010, accessed on 2022 at the following address

[1509] Le Monde with AFP, " Sam Bankman-Fried, former CEO of cryptocurrency platform FTX, pleads not guilty à New York", 2023, Le Monde.fr, see also Wikipedia contributors, "*Mt. Gox*", available at

production of computer chips[1510] or to certain computerized and socially centralized Internet standards, which Bitcoin exploits and on which it may depend[1511] . This means that, in theory, these latent levers of dependency could one day be activated and articulated by certain actors (companies, institutions, governments) in order to destabilize this network. In practice, it would be quite complex for actors to successfully coordinate the activation of such levers in order to discredit the trust placed in all or part of this network and its ecosystem of actors. Aware of these currently untapped dependencies and threats, some players in the Bitcoin community are continually innovating to reduce these IT and social dependencies, particularly on the ever-pivotal Internet infrastructures (TCP/IP, Internet platforms, etc.). For example, since August 2017, it has been possible to operate a satellite-based Bitcoin node via the acquisition of a dish directly connected to the satellite of Canadian company Blockstream[1512] . The latter synchronizes the valid blocks of the Bitcoin blockchain in real time and then transmits this data to each satellite dish of this parallel network, which is now independent of the Internet, because it is satellite-based. More recently, since July 2022, it has been possible to send fractions of bitcoins ("satoshis") via the Lightning Network[1513] directly from all types of cell phone, a solution currently being deployed in Africa[1514] . In this way, Bitcoin seems to be gradually becoming less dependent on the Internet, a trend that will need to be confirmed in the future to ensure its IT resilience over the long term.

Focus 3: A new economic and accounting incentive and valuation system

Once validated, blocks currently create and release 6.25 new bitcoins every ten minutes[1515] . This amount, known as "*genesis block compensation",* encourages users to carry out the calculation work mentioned - and detailed in Appendix 6 - in order to generate new, compliant blocks. Every four years or so, the number of bitcoins that can be mined, i.e. issued per block, is halved (a phenomenon known as "*halving"*). This programmed cryptographic scarcity explains the a priori sustainable rise in the value of a bitcoin over time[1516] , as supply theoretically becomes lower than demand thanks to this "halving" phenomenon.

[1510] For the entire IT industry, including the Bitcoin infrastructure, the outbreak of a conflict in Hawaii could lead to a probable disruption in the supply of computer chips, particularly for certain *integrated circuits* (*ASICs*). Mining companies rely on TSMC (an *oligopoly* with a market share of over 50%), which currently produces a large quantity of these components, which are essential to the Bitcoin infrastructure.) Bitcoin's material dependence on these chips and their suppliers is a point of dependence subject to the vagaries of its geopolitics and nearby geography. V. Wikipedia contributors, "Taiwan Semiconductor Manufacturing Company", 2022, available at

[1511] De FILIPPI Primavera, "Blockchain and the Law", 2017, *op. cit,* "*Protocols like Bitcoin ultimately rely on TCP/IP to function.*", location 968 of 7004.

[1512] Consult the *Satellite Kits* on the Blockstream Store at the following address, as well as the dedicated interactive map

[1513] V. Appendix 6, Focus 1.

[1514] MAIRE Vincent, "Bitcoin (BTC): Machankura makes it possible to receive satoshis without an Internet connection", 2022, available at

[1515] As a reminder, to be accepted into the chain of previous blocks, new blocks must include a valid *Proof of Work.*

[1516] In 2008, the reward for each bitcoin block was 50 units, issued every ten minutes. This reward was halved automatically on November 28, 2012, to 25 bitcoins issued every ten minutes, then halved again on July 9, 2016, to 12.5 bitcoins, and again on May 11, 2020, to 6.25 bitcoins. At

an initially artificial mechanism adopted 14 years ago[1517] , and now assumed by the community to be immutable. In around 2140, this programmed reduction in the reward per block will come to an end, and validators ("miners") will therefore be remunerated exclusively by charging fees on the validation of user transactions[1518] . In this respect, the user who sends a bitcoin transaction pays a commission on the transaction, which will be retained by whoever finds the next block. The payment of these fees by users encourages miners to include the transaction in a new block more quickly (the higher the fee, the faster the transaction will be processed, within the limit of 10 minutes between each block). It's also worth noting that the electrical expenditure required by miners to find the above-mentioned mathematical solution (which is a *winning hash* among all the other *hashes calculated*), is intuitively perceived as a waste of energy[1519] . In reality, these supposedly pointless computations represent an electrical cost that underpins the status and social and monetary value accorded to Bitcoin in comparison with today's fiat currencies (which are not based on a unified, transparent energy cost model). In parallel with this process of programmed monetary issuance, stable over time thanks to the protection of its developer community, it is essential to remember that there will never be more than 21 million Bitcoins issued, which means that its total emissible quantity is limited in number and time, in the same way as the theoretical quantity of gold available in the world[1520] .

From an accounting point of view, the gradual increase in the number of bitcoin transactions[1521] , including for economic transactions, could enrich the double-entry accounting[1522] which is

---

By May 2024, this same reward will be 3.12 bitcoins issued every ten minutes. This planned, constant and automatic scarcity in the production of new bitcoins leads to a theoretical and gradual increase in its value every four years, as with gold whose quantity available and in circulation is limited, which explains the nickname "*digital gold"* attributed to bitcoins.

[1517] It is emphasized that these algorithmic and physical (machine) mechanisms whose purpose and effect is to generate digital rarefaction are initially 'artificial' in the sense that they are socially programmed and desired by its community (unlike gold, for example). However, this rarefaction gradually becomes 'pure' and no longer 'artificial', as the people behind these mechanisms no longer have control or influence over these concepts, which ultimately function at the service of the entire open network, which consequently becomes a digital commons.

[1518] If this system of programmed cryptographic rarefaction delivers on its promise by 2140, every fraction of bitcoin issued will become very rare and consequently high-priced, guaranteeing validators/miners a reliable and sustainable economic income thanks to transaction fees between users as their sole source of remuneration (because after 2140 there would be no more "*genesis block compensation"*).

[1519] V. Appendix 6, Focus 1.

[1520] This quantity is estimated to be the equivalent of a soccer stadium alone, which explains gold's scarcity and therefore its high price. However, it is important to distinguish between *relative* and *absolute scarcity*. Gold is *relatively scarce*, because its total quantity is limited and subject to the means of extraction (mines, machines), while bitcoin is *absolutely scarce*, because its quantity is mathematically limited and computer-sealed, meaning that attempting to use more computers to extract more than 21 million bitcoins is theoretically impossible. Satoshi Nakamoto explains the choice of 21 million bitcoins in the following terms: "My choice for the number of coins [bitcoins] and the distribution program was an educated guess. It was a difficult choice, because once the network is launched, it's locked and we're stuck with it. I wanted to choose something that would make the prices similar to existing currencies, but without knowing the future, it's very difficult. I ended up choosing an intermediate solution. If bitcoin remains a small niche, it will be worth less per unit than existing currencies. If you imagine it being used for a fraction of world trade, there will only be 21 million coins for the whole world, so its value per unit will be much higher", in *Gmail - Questions about Bitcoin*, accessed on October 27, 2022, at [1521] It is possible to observe in real time from 2010 until today the undeniable growth in transactions carried out on the bitcoin blockchain. See Blockchain.com | "Charts - Total Number of Transactions".

[1522] Wikipedia contributors, "Double-entry accounting", 2022, available at

Today, accounting is standardized for all legal entities. Indeed, accounting records, whether paper or digital, can be easily manipulated and altered by third parties, leading to errors that can compromise the balance of an accounting system. The use of the Bitcoin blockchain and bitcoins could help to reduce the impact of human error by automating certain types of transaction and providing more accurate and easily verifiable data. Consequently, incorporating bitcoins into "*double-entry accounting*" could improve the accuracy, transparency and efficiency of certain accounting processes. This concept of "*triple-entry accounting*"[1523] is a concept primarily made possible by the Bitcoin public blockchain. This new accounting principle thus proposes a third component
3.0: a public blockchain. Because only the Bitcoin public blockchain seems incorruptible, i.e. likely to be around in a few decades' time, its IT transparency would enable it to be used as an accounting and financial auditing system. Indeed, each bitcoin debit could be used to time-stamp, track and even issue credits linked to other assets (euro, other stable or unstable crypto-assets) which would be anchored on this cryptographic data chain to leave an unalterable accounting and digital trace. This would supposedly considerably reduce certain accounting errors and fraud, while ensuring real-time accessibility to every accounting entry (debit, credit). Beyond the digital identity proofs mentioned in this research, a relevant use of triple-party accounting would be to certify professional and commercial (not personal) accounting information, such as annual accounts or reserve requirements specific to commercial banks[1524] . This would provide reliable and more transparent evidence of the approval of such information, thereby reinforcing the accountability, trust and credibility associated with financial transactions, in a context - of crisis of confidence - that is digital. Although triple-party accounting is primarily applicable to the Bitcoin blockchain, which alone possesses a degree of pure decentralization in the sense of this study[1525] , its emergence is likely to face numerous social, political and legal barriers mentioned throughout this study. In order to adopt this triple-entry accounting principle, the use of certain layers and protocols complementary to Bitcoin's, such as the "Lightning Network", "Taro" or more recently "Ordinal"[1526] and "Bitcoin Stamps"[1527] studied below, could help overcome some of these currently omnipresent obstacles. In concrete terms, the recent Taro update and subsequent developments will make it possible to anchor administrative and accounting documents directly on the Bitcoin blockchain, while enabling loan and credit transactions to be carried out directly on this same blockchain (still with the intervention of legally supervised 2.0 and 3.0 financial institutions). This

[1523] Bitcoin.fr, "An application of Bitcoin: triple-entry accounting," 2015, available at bitcoin.fr
[1524] Banque de France, "Les réserves obligatoires", 2022, available at the following address
[1525] See *above,* I, Title 2, 2.1.3.
[1526] See below.
[1527] See below.

could pave the way for the advent of triple-entry accounting, redefining the contours of our current accounting principles. Finally, it is emphasized that the gradual increase in the price of bitcoin since its launch is encouraging economic players to join the network to secure it, while financing its algorithmic and infrastructural improvements. It's a virtuous circle of financing that contributes to the creation of a rare cryptographic commons that benefits humanity.

Focus 4: Towards a multimodal, emerging monetary (Lightning Network), financial (Taproot & Taro) and storage (Ordinals/Bitcoin Stamps) network

To ensure that third parties and malicious users cannot spend other users' bitcoins by creating non-compliant transactions, the Bitcoin protocol uses public key cryptography to ensure verification of digital signatures. In this system, each user has a unique address associated with a pair of public and private keys, which are stored in a dedicated bitcoin wallet (usually via a mobile application, software on a computer or a dedicated USB key, all dedicated to this purpose). Only the user with a private key can sign a transaction to send all or part of his or her bitcoins to the bitcoin address - public key - of another Internet user. Thanks to this system, each user is able to exchange bitcoins with other users at a relatively low cost and validation time compared to the banking sector[1528] . In this way, the Bitcoin protocol already provides an efficient payment system for large-value transactions. While a user can theoretically also carry out small-value transactions ("microtransactions"), in practice the applicable transaction fees often deter users from carrying out such transactions, as the fees are higher than the amount of the transaction. This impossibility of carrying out transactions of a few cents - in fractions of a bitcoin (microtransactions in "satoshis") - was already a problem for some users in 2015. In effect, this prevented bitcoin from being considered a currency. The ability to carry out microtransactions is therefore essential for many exchanges, such as the purchase of basic necessities (food, housing). Without a suitable solution for the Bitcoin network, users have to wait tens of minutes, sometimes hours, before they can be sure that their transactions are registered in a valid block. Since these payments of less than a few euros equivalent in satoshis are not very suitable on the main Bitcoin network ("*Layer 1 - L1*") due to the high costs involved, a secondary computer network ("*Layer 2 - L2*") was devised in 2015 and implemented from 2017 to

[1528] In fact, it is emphasized that fees fluctuate automatically according to certain parameters of the Bitcoin network. However, users can always decide how much they want to pay the miners for their transaction to be validated in the nearest block (at best in ten minutes, and otherwise after several blocks, e.g. 6 blocks, i.e. a 60-minute wait).

answer to this problem: the *Lightning Network - LN*[1529] . The[1530] LN is simply a P2P protocol whose distinctive feature is that it is cryptographically attached to the Bitcoin blockchain (L1). In this way, LN can be seen as an outsourcing computer protocol (L2)[1531] dedicated to carrying out microtransactions in fractions of bitcoins, whose sub-unit of account is called a "*satoshi*"[1532] . Now up and running and being adopted by tens of thousands of people worldwide, the LN not only enables users to carry out transactions of any amount, in the same way as a currency (in this case independent and automated), but also to spend a fraction of these assets as a store of value, which is impossible for gold, for example, which cannot be easily fractionalized and then spent. In other words, LN makes it possible to spend fractions of one's digital gold (in satoshis), an action impossible with gold bullion. As a result, Bitcoin and its protocols (L1 and L2) enable value to be retained over time, while allowing fractions of bitcoins to be spent instantly, virtually free of charge and without a trusted third party. In this way, the Bitcoin blockchain (including LN) represents a (r)evolution for the online payments sector. However, the Lightning Network remains an experimental ("*beta*") protocol[1533] with certain theoretical security flaws already identified[1534] , although not yet exploited. LN is also partially centralized from an IT and social point of view (see Appendix 7), simply because it was launched relatively recently. If its operation is designed to be progressively decentralized like the Bitcoin blockchain (L1), this will require time and a certain network effect, which are incompressible, entailing an initial need and degree of trust (third parties offering simplified, and therefore rather centralized, access to this L2). While this network has been growing since its launch, it must be remembered that it cannot be implemented and used by everyone in its current state (2023). On the one hand, it is not suitable for all situations, i.e. it does not meet all payment needs.

[1529] MICHALAKIS Fanis, Youtube channel, available at the following address

[1530] To understand the rudiments of this protocol adjacent to the Bitcoin blockchain see the following translation, free from English, "The Lightning Network is a decentralized system of high-volume instant micropayments that eliminates the risk of delegating custody of funds to trusted third parties. For example, Bitcoin, the world's most widely used and valuable digital currency, allows anyone to send value without a trusted intermediary or custodian. Bitcoin contains an advanced scripting system that allows users to program instructions for funds. However, there are drawbacks to Bitcoin's decentralized design. Users have to wait tens of minutes or even an hour to be confident that their transactions will not be reversed. Micropayments, or payments of less than a few cents, are inconsistently confirmed, and fees make such transactions unviable on the network today. The Lightning Network solves these problems. It is one of the first implementations of a multi-party smart contract (programmable money) using Bitcoin's built-in script.", "Layer 2 | Lightning Network." (2022), in *MIT Digital Currency Initiative*, available at

[1531] High-value transactions (e.g. over €100 bitcoin equivalent) are carried out on *Layer 1*, and low-value transactions on *Layer 2* (Lightning Network).

[1532] *Satoshis* are fractions of bitcoins, the same asset but simply a more precise unit of account. As of 14/08/2022, 1 *satoshi* is equivalent to 0.00000001 bitcoin or 0.00024 dollar cents, see the online conversion site at

[1533] Lightning Labs, "Announcing lnd 0.15 beta: To Taproot and Beyond!", 2022, available at

[1534] SGUANCI Cosimo, "Mass Exit Attacks on the Lightning Network", 2022, University of Illinois at Chicago Chicago, available at

IT challenges mentioned in this research (network centralization and/or congestion, rising costs, hacker attacks, etc.)[1535] .

In 2021, a new Bitcoin protocol update proposed the implementation of "*Taproot*", a system enhancement that combined several Bitcoin protocol optimization proposals ("*Bitcoin Improvement Proposal - BIP*")[1536] . These upgrade proposals were implemented in November 2021 and then progressively deployed within the software and applications of the Bitcoin ecosystem, i.e. joined by digital wallet software as well as exchange platforms, which for the record enable the conversion and/or exchange of bitcoins. In concrete terms, Taproot's implementation has not only enhanced Bitcoin's scalability, but also contributed to its security, confidentiality (pseudo-anonymity) and transaction flexibility. In the next few months or years, Taproot will pave the way for the deployment of smart contract, DAO, NFT or stablecoin concepts directly on the Bitcoin blockchain (see the complementarity with the "*Taro"* protocol below). As a result, numerous technological building blocks could eventually be attached to Bitcoin to build associated services of all kinds, such as decentralized social networks, distributed online browsers (P2P)[1537] , etc.

With multiple consecutive updates, including "*Segwit" in* 2017[1538] , skilfully orchestrated by its community since they are compatible and chronologically interwoven, the launch of a new protocol in the making was announced on April 5, 2022 :
"Taro". Announced in April 2022[1539] , this new protocol would, to put it simply, diversify Bitcoin by making its L1 and L2 compatible with multiple use cases currently inaccessible to its users. For some, Taro would represent a serious achievement for the Bitcoin project and ecosystem: its protocol would become multifunctional, multimodal, and no longer monofunctional as at present. It would thus evolve from an exclusively monetary digital infrastructure to an eclectic digital infrastructure[1540] . For financial institutions, the implementation and adoption of Taro would probably represent, if they live up to their promises, an immense challenge to some of their current business models. In concrete terms,

---

[1535] V*, supra*, I, Title 1, 2.3.2
[1536] When developers want to make an update to the Bitcoin protocol, they submit *BIPs.* on the dedicated Github account
[1537] In November 2022, the *Impervious* browser made its appearance. This is a suite of P2P tools for communications and payments, integrated directly into users' Web browsers. This browser already natively integrates the Lightning Network, decentralized identity standards (did) and the ION protocol we mentioned earlier. In short, this browser confirms our hypothesis that it's the next step towards a sophisticated, native digital identity built directly on the Bitcoin blockchain (INAS). For more information, please visit
[1538] Investopedia, "What Is Segregated Witness (SegWit)?", 2022, available at
[1539] "We see Taro as a milestone in the 'bitcoinization' of the dollar, achieving the best of both worlds: 1) issuing assets like stablecoins on the most decentralized and secure blockchain, bitcoin, and 2) enabling users to transact on the fastest and lowest-cost global payment network, Lightning," "Announcing Taro: A New Protocol for Multi-Asset Bitcoin and Lightning," April 5, 2022, in *Lightning Labs*. Available at
[1540] "Who brings together a great variety of tendencies, who chooses from very diverse categories", in *Larousse 2022*. Definitions : eclectic - French dictionary www.larousse.fr

Taro would enable all Internet users, organizations and Bitcoin users to issue their own assets directly on the Bitcoin blockchain, with near-instantaneous efficiency, high volume capacity and relatively low transaction costs. If, thanks to Taro, Bitcoin were to achieve this decentralized digital Grail - first monetary, then eventually financial and industrial - central banks and, more generally, institutions the world over would be called into question in terms of their respective roles and usefulness. This digital transition to a common 3.0 monetary and financial universe would enable the renegotiation of certain often unfavorable power relationships between certain developing countries and their unstable currencies (Venezuelan Bolivar, Turkish Lira, Lebanese Lira), and the stronger currencies of developed countries. In this respect, the recognition of bitcoin as a legal tender in El Salvador is a first step towards this utopian future (*see* Appendix 5). While it is difficult to maintain that Bitcoin will be able to accommodate all digital transactions in the near future, due to its inability to meet all of society's complex needs, it does seem to provide a relevant foundation for all transactions with high social, identity, financial, monetary or accounting added value. For the time being, Taro is in the early stages of development, with the Lightning Network providing a more advanced foundation, but also still under construction. For the time being, there is no guarantee that Taro will be successfully implemented and deployed in the near future, as difficulties and unforeseen events are constant and recurring risks in complex software development processes, because here they are interwoven and open.

In early 2023, a new feature - unintentionally enabled by the aforementioned Taproot update - emerged: the "*Ordinals*" protocol[1541] . This concept proposes the creation of what amount to NFTs stored directly within Bitcoin blocks. As a reminder, each bitcoin is made up of small units, satoshis, and these can now - thanks to the *Ordinals* protocol
- be individually 'burned' with content such as images, videos or text, to create unique digital artifacts that circulate on the Bitcoin blockchain. They can then be stored in specific Bitcoin wallets and transferred using conventional Bitcoin transactions. These engravings ("*inscriptions*")[1542] or NFT specific to the Bitcoin blockchain, are therefore assumed to be as durable, immutable, secure and decentralized as the infrastructure on which they are based (L1).

As a result, these multiple consecutive updates seem to be gradually moving towards and converging on a form of diversification - voluntary for some and latent for others - of the possible uses of the Bitcoin protocol, without abandoning its primary purpose, which is to

[1541] View these Bitcoin blockchain-anchored entries in real time, in principle for as long as they exist, via the following website. A few months after Ordinals, another protocol with similar aims was born: "*Bitcoin Stamp", which is* more costly to operate, but more reliable and resilient for anchoring information within Bitcoin blocks.
[1542] To illustrate the previous footnote in real time, here's an example of a *registration* on *Ordinals* and an example of a *stamp* on *Bitcoin Stamps*.

currency. Bitcoin would thus eventually become a universal digital infrastructure, enabling all types of players to immutably anchor more or less complex, but always equally immutable and valuable, datasets. Thus, Bitcoin currently retains its relevance in at least two areas, namely the financial sector and that of proof of datasets. The proof-of-data use case can be applied to many sectors, but this requires compliance with current legal rules, a quest for legal conformity that is not - and probably won't be - a priority for the developers of the Bitcoin blockchain, who are seeking above all to ensure its resilience and IT and social decentralization.

Focus 5: Pseudo-anonymity as a guarantee of resilience for Bitcoin

Originally, accessing the Bitcoin network did not require the creation of an account with a specialized online service (as is the case today)[1543] , but simply the download of a specific software program (digital wallet)[1544] , followed by the purchase of Bitcoins from a natural or legal person who owned them. Anonymity was thus fundamental to the launch of Bitcoin, i.e. a technical and community standard by design. In concrete terms, a bitcoin address corresponds mathematically to a unique public key, and looks like this "*bc1qq2zpjy6qs7cxm25779wutw8w9450hzxfmdwsw7*"[1545] . Each fraction of bitcoins cryptographically belongs to the person who owns the associated private key, enabling him or her to sign (send) transactions with it. Through their Bitcoin-compatible virtual wallets, each person can generate and own several such addresses, each with its own balance. This makes it more or less difficult to know which user owns which amount of Bitcoins, depending on the efforts made by the user to avoid being identified retrospectively through the use of his or her addresses. With the ingenious and reliable operation of these addresses and cryptographic signatures, the pseudo-anonymity by design of the digital (crypto)financial identity of bitcoin users could remain within this ecosystem for a few more years. Nevertheless, since around 2017, international regulations require prior identification for the purchase or sale of bitcoins by individuals, and sometimes specific registration for legal entities operating in this sector (which will probably be the norm within a few years), as has been studied in this research (*see* also Appendix 14). Ultimately, the pseudo-anonymity inherent in Bitcoin's operation is being eroded year by year in the face of strict LCB-FT standards and regulations. It has to be said, however, that this struggle is not always based on a clear understanding of Bitcoin.

[1543] Initially (before 2012), no email address, username or password was required to hold or spend bitcoins. With the boom in its adoption and use, a majority of users acquire crypto-assets via crypto-asset exchange platforms, today all subject to systematic identification in accordance with banking and financial law. This trend is growing stronger every year in most international jurisdictions.

[1544] Download Bitcoin. 2022. Bitcoin.org, *v. supra*, II, Title 1, 1.3.1.3

[1545] Each bitcoin address is publicly visible on a visual interface directly linked to this blockchain, to enable better reading of its information (addresses, transactions, current balance). To view this address, please consult the following link

reasonable and proportionate to the risks it poses to the majority of honest bitcoin users, but rather on a desire for over-identification that would contribute to progressively altering the perception of the value of bitcoins by discriminating against them, as already assumed in the course of this thesis[1546] .

Focus 6: Bitcoin as a universal capital and social commons

The Bitcoin protocol is a tool that promotes the online freedom of individuals by enabling them to communicate, express themselves and undertake business freely. The U.S. Supreme Court has confirmed that the "*Proof of Work* - PoW" mechanism, presented in Appendix 6, is protected by the fundamental right to freedom of expression, under the First Amendment to the U.S. Constitution[1547] . This recognition underlines the importance of freedom of expression in the digital world, and reinforces the legal and social recognition given to public blockchains as cryptographic guarantors of this freedom. The social contribution of the Bitcoin system - enabling a new form of bancarisation 3.0 - is considerable, and since 2010 has gradually enabled the purchase of goods and services online[1548] . Eventually, it could also offer the possibility of creating decentralized digital identities to access various online services such as social networks 3.0, insurance 3.0, credit 3.0, and gradually introduce its triple-entry accounting to these services. The Bitcoin blockchain offers unprecedented protection for honest users against censorship and digital manipulation, although it will always allow a dishonest minority to carry out illegal actions (a problem that cannot be solved or avoided by any existing technology). So, in reality, Bitcoin has a mainly positive impact on society, facilitating online transactions, protecting the rights of Internet users and providing opportunities for innovation in key sectors such as economic and financial services.

In addition, Bitcoin is a non-political, socially agnostic computer protocol that contributes to "[1549] , not to say to question its very foundations. Through its absolute openness, it introduces for the first time, thanks to its ingenious economic system coupled with its IT decentralization, the notion of digital scarcity on the Internet. We need to perceive it as a tool for emancipation in the service of certain fundamental human rights, such as the right to privacy, digital integrity and even informational self-determination mentioned in this research. Thanks to its usefulness, neutrality, cryptographic security and seemingly unstoppable growing community, Bitcoin seems to be a (r)evolution that will stand the test of time, i.e., a system that only needs time for the majority of Internet users to become aware of its unparalleled digital and social value proposition (compared to other crypto-nationals).

[1546] See *above*, I, Title 2, 2.5

[1547] DANIEL Aaron, "New York's Proof-of-Work ban violates Bitcoin miners' right to free speech," in *Bitcoin* Magazine, available online, free translation from English "Supreme Court case law shows New York's moratorium on proof-of-work mining violates bitcoin miners' First Amendment rights."

[1548] HOWELL James, "What Is Bitcoin Pizza Day?", 2023, in *101 Blockchains*, available at.

[1549] De MOMBYNES Yorick, Lecture at Surfin' Bitcoin, 2022, "Depoliticizing currency", YouTube. Accessed at

assets). There's no doubt that in the decades to come, and provided that certain regulations do not hinder its use (total prohibition, systematic and disproportionate identification of all Bitcoin holders), Bitcoin will probably eventually be perceived as an IT infrastructure promoting individual emancipation, in response to some of the ills of an ultra-connected society already subject to constant surveillance of Internet users.

In a nutshell:

With this in mind, we can suggest a three-stage summary of what the Bitcoin protocol will be in 2023, what it probably won't be by 2025, and what it might be in the longer term, i.e. after 2025. These postulates and conjectures are based on the ideas developed in this research and finally summarized in this table:

<table>
<tr><th><u>What Bitcoin is</u>
Findings since 2020 (High Objectivity)</th><th><u>What Bitcoin won't be</u>
Findings to 2025 (Relative objectivity)</th><th><u>What Bitcoin could become</u>
Conjectures after 2025 (Low Objectivity)</th></tr>
<tr><td>The currency of the Internet: Majority societal recognition</td><td>A digital infrastructure that complies with the legal texts studied : Majority societal recognition</td><td>A legally and globally recognized currency: Relative probability</td></tr>
<tr><td>A legally and globally recognized currency: Minority societal recognition</td><td>A privileged asset for financing illicit activities (money laundering, terrorism): Minority recognition by society</td><td>A multimodal monetary, financial, storage and asset tokenization protocol: High probability</td></tr>
<tr><td>A resilient, unchanging digital commons: Majority societal recognition</td><td rowspan="2">An IT system that is flexible and adaptable to changes in its socio-economic environment: Mainstream societal recognition</td><td>An open and trusted registry and IT platform for INAS : Relative probability</td></tr>
<tr><td>A legally and globally recognized financial asset: Majority societal recognition</td><td>A digital infrastructure to support the energy transition[1550] : Relative probability</td></tr>
</table>

[1550] V. Appendix 6, Focus 1.

Caption:
Minority societal recognition = success dependent on individual recognition by a minority of Internet users and citizens, but without collective recognition from the public and private sectors.
Majority societal recognition = success depends on majority individual and collective recognition by Internet users/citizens and by the public and private sectors.
Relative probability = success depends on partial and uneven individual and collective recognition by Internet users/citizens and public authorities.
Probability high = success dependent on recognition individual by coupled with collective recognition by public authorities.

Appendix 4: The utopia of a self-proclaimed blockchain state (Liberland)

As previously mentioned, advocates of blockchain technologies initially tend to trust only programming and mathematics thanks to algorithms and cryptography. This desire for disintermediation concerns all trusted third parties, including governments. Blockchain technologies make it possible to imagine social and economic relations that are supposed to be totally disintermediated ("decentralized"), for example with a nation using all the new disruptive technologies at its disposal. This community dream has been imagined by techno-libertarians and put into practice via a full-scale project that is now accessible to all with just a few clicks: "*Liberland*". The Free Republic of Liberland is a 7 km² island located on the western bank of the Danube, between Croatia and Serbia, sharing a land border with the former and a river border with the latter. Liberland was (self)proclaimed on April 13, 2015 by its President Vít Jedlička. While Croatia does not recognize the territory of Liberland as its own, it paradoxically declares that it is nobody's land ("*terra nullius*")[1551] . This implies that it should belong either to Serbia or to Croatia, which deviates from this position by considering the territory as a border for historical and political reasons. For the past eight years, this self-proclaimed state has been developing a legal framework comprising a constitution[1552] and laws[1553] , all inspired by libertarian principles[1554] . It's worth noting that this blockchain-programmed constitution - supposedly open - has so far only legal recognition in the eyes of the citizens of this territory, which is not officially recognized under international public law. The new IT component represented by blockchain (see below) gives rise to a dematerialized state, supposedly decentralized, awaiting appropriation of an unclaimed territory. This new movement led by technophiles and libertarians aims to establish direct democracy using blockchain technology for its representative elections. The aim is to guarantee absolute transparency in the electoral process, by enabling voters to cast their ballots directly via a blockchain that is supposedly public but in reality state-owned (so it's a hybrid blockchain), ensuring the verifiability of results. In addition, a parliament is elected to work with this direct-democratic system. On the official Liberland website, it is stated that in 2022, over 500,000 people are awaiting citizenship, and that around 1,000 of them already have Liberland citizenship. Only 17,000 Liberland citizens could one day become physically resident on the 4 km² available territory[1555] . Liberland is already producing its titles

[1551] This term refers to "*territory without master*". It is a term used in public international law to describe an area that may be inhabited but does not belong to a state, meaning that the land is owned by no one. According to some jurists, this principle can be used to justify the claim that territory can be acquired through occupation by a state.
[1552] Liberland. 2022. "The Constitution of the Free Republic of Liberland. liberland.org
[1553] Liberland. 2022. "The Articles of the Provisional Government of the Free Republic of Liberland. liberland.org
[1554] Its constitution and laws were inspired by the tradition of classical liberalism, with a strong emphasis on property rights and individual freedoms.
[1555] BINSKY Drew, "The Country That Doesn't Yet Exist (Liberland)", 2022, YouTube

identity cards and passports), which are not recognized internationally, for the sole benefit of its e-residents and citizens (see below). Ultimately, Liberland would provide each citizen with tokenized citizenship in the form of one or more digital tokens directly accessible in their crypto-asset wallet, i.e. through a citizenship NFT[1556] . For this purpose, the use of "*Soul Bound Token*"[1557] seems to be a preferred avenue in 2023. This tokenization of the digital identity of Liberland citizens (close to the INAS studied) does not, however, seem to be moving towards compliance with the RGPD or the eIDAS Regulation, which also raises questions about the compliance of this self-proclaimed micro-nation in the face of other Regulations or amendments currently being adopted (MiCA, TFR, Data Act). The state's budget seems minimal, with just four ministries and a justice system that could be decentralized thanks to the Kleros protocol.

In 2015[1558] , Liberland announced the official adoption of Bitcoin as its national currency[1559] , making it the first (self-proclaimed) state in the world to take such a decision. This initiative was therefore implemented ahead of El Salvador[1560] , which adopted Bitcoin as its legal currency in 2021. However, in March 2019[1561] , Liberland launched its own crypto-currency, the "*Liberland Merit - LLM*
", which was first enshrined on the "*Bitcoin Cash*" public blockchain[1562] , then finally abandoned in 2020[1563] . Following this failure, Liberland decided to adopt a new blockchain infrastructure, named "*Polkadot*"[1564] , which is inspired by and linked to the public Ethereum blockchain[1565] . This infrastructure supports smart contracts and aims to create an economic incentive similar to that of the Bitcoin public blockchain, notably by instituting a supposed programmed scarcity of tokens in circulation on this network. In reality, this process of artificial scarcity eventually becoming pure over a long period of time seems impossible to achieve[1566] , something that only Bitcoin has succeeded in doing to date. In fact, Liberland seems to have been in its infancy for several years.

[1556] The citizenship token will contain: a photo of the citizenship ID, a link to the owner's Liberland account (*v.* experimental e-resident account), the number of *Liberland Merits (LLM)* staked in the citizenship and the history of that particular citizenship token, in *docs/Blockchain Strategy.md at master* - liberland/docs. GitHub

[1557] See *supra,* I, Title 1, 2.3.1.1.

[1558] NewsBTC, "Liberland Chooses Bitcoin as National Currency," 2015, available online.

[1559] That's seven years before El Salvador, although Liberland is not yet recognized as an official country, unlike El Salvador.

[1560] V. Appendix 5.

[1561] DIXON Brent, "Liberland's Merit Token Built on Bitcoin Cash," 2021, available at.

[1562] This is a kind of "*fork*" of the original Bitcoin blockchain. Today, this copied blockchain is little recognized and adopted by the original Bitcoin community.

[1563] "In 2020, we decided to transfer our blockchain-based e-governance concept from EOS.IO technology to our own Polkadot ecosystem, which will be launched in the fourth quarter of 2021", in *The free republic of Liberland ministry of finance*, 2021, Liberland, p.3, available at.

[1564] *Polkadot* is a communication protocol and a so-called "*multi-chain"* platform, enabling all types of blockchain (and their applications) to communicate with each other. Available online

[1565] It is possible to observe the transaction history of this blockchain via the following address (link visited 02/01/2023) [1566] As a reminder, it is emphasized that these algorithmic and material mechanisms whose purpose and effect is to generate digital rarefaction are originally artificial in the sense that they are programmed and desired (unlike the availability of gold, for example). However, this rarefaction gradually becomes *pure* and no longer *artificial*, as the people behind these mechanisms no longer have control or influence over these concepts, which are thus at the service of the entire network and therefore of the common good.

regarding its deployment strategy for its blockchain and digital token[1567] , which are essential to its supposedly resilient and decentralized 3.0 digital governance model. Indeed, as regards both its governmental DAO and its LLM token, and more generally its official blockchain (see hereafter the "*Liberland Smart Chain - LSC*"), it appears that its digital strategy still remains unclear and ambiguous, despite the progress it has announced. At the beginning of 2023, the blockchain deployed by Liberland suffered from an apparent lack of IT and business development, as the following second screenshot shows. By the end of 2021, Liberland had also announced the development of its own Metaverse, the "*Liberland Metaverse*"[1568] , with the aim of strengthening its online presence and, above all, attracting new foreign capital. By the end of 2023, this self-proclaimed e-state's ambition is to gradually deploy these multiple technical components to serve its e-residents and citizens. In this respect, it is possible that Liberland will take up the subject of INAS in order to offer its citizens the possibility of connecting to its online services, following the example of company management, which can be registered at Liberland[1569] . Although this hypothesis is only a fiction to date, such an event would make Liberland a leader in the massive use of 3.0 technologies. However, the theoretical use of these 3.0 technologies would have to be compared with their actual use, which could quickly lead to disillusionment and even abuse. To illustrate, each e-resident does not have an equal right to vote in Liberland, but only the power to vote according to the amount invested in Liberland, thus creating an ultra-capitalist system that is a potential source of future social conflict.

Finally, while Liberland in 2023 may represent a political utopia for citizens disillusioned with their original nationality, its progressive social and IT development makes this experiment a novel project in an era of almost total dematerialization of social and administrative interactions. While Liberland represents an ecosystem that is particularly inclined to move towards the advent of a universal identity, and as such should be followed with attention, it remains in reality a legally and politically closed ecosystem circumscribed to its citizens, contrary to the Proof of Humanity protocol[1570] . According to an academic article published in 2016 in the Chicago Journal of International Law, international legal recognition of Liberland depends[1571] strictly on its recognition by a sufficient number of states, which recognize each other by

---

[1567] Liberland is on the lookout for developers, a now highly prized resource that Liberland seems to be having trouble attracting in light of the advances sprinkled throughout its publicly accessible IT development on its Github account. *Call for Developers*. January 13, 2022, liberland.org

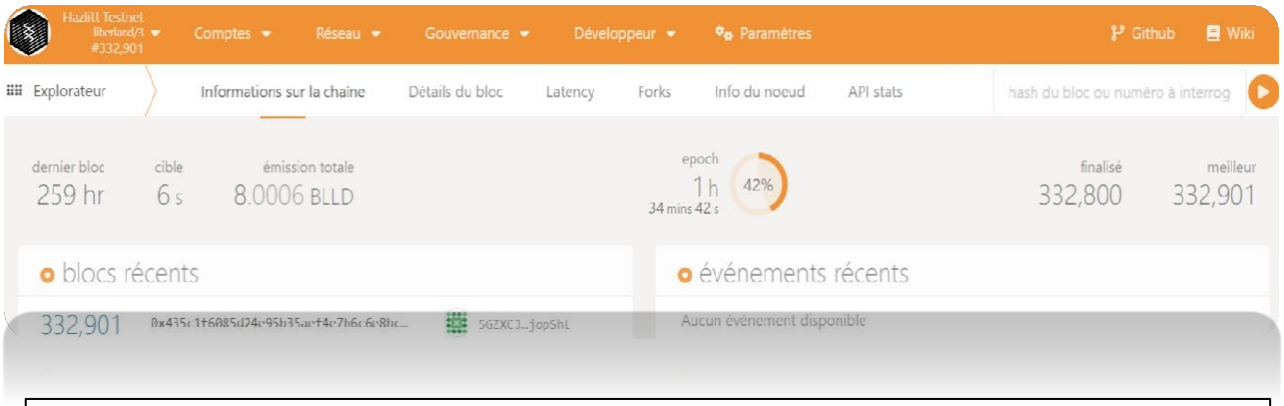
[1568] "World Liberland Metaverse". For more information, visit the following address

[1569] All *e-residents* have access to an official Liberland platform enabling them to offer products and services such as company registration in Liberland. Available at the following address

[1570] See *above,* I, Title 2, 2.9

[1571] [...] there are two potential routes by which Liberland could gain recognition. Firstly, Liberland could convince the international community that the territory it claims is terra nullius due to the informal renunciations by Serbia and Croatia of their title to this territory. Liberland would then have to meet the Montevideo criteria. However, Liberland would not be able to satisfy a strict application of the Montevideo criteria, as it does not have a permanent resident population, a government or a territory of its own.

elsewhere. Even if Liberland were to obtain partial legal recognition, it would still be forced to comply with multiple regulations before being able to establish relations with countries respecting international rules. This constraint could hamper Liberland's libertarian ambitions, as its physical territory has remained inaccessible for almost 10 years. In the absence of international recognition by developed countries in the future, it is highly likely that Liberland will concentrate on trade relations with developing countries[1572] in the hope of building alternative international relations strong enough to demonstrate that its utopia was not just a dream. In the near future, perhaps within a decade or two, the world will witness either the greatest scam and attempt to create a new country, or the emergence of a new 3.0 state forged from scratch by individuals sharing common social aspirations and varied ideals.



Legends and explanations:

The two preceding photos, representing a scan of a Liberland e-resident card and then a screenshot of the Liberland (LLC) blockchain on 02/01/2023. Combined, they give an idea of the development and link that would exist between Liberland's claimed identity credentials and its supposedly public, decentralized and incensurable blockchain. The integration of a microchip in these credentials would make it possible, in the not-too-distant future, to carry out immutable acts recognized by the Constitution and laws of Liberland.

The international community has viewed Liberland's claim to statehood with considerable skepticism. [...] the international community has viewed Liberland's claim to statehood with considerable skepticism. It is unlikely that the international community will choose to apply the less stringent version of the Montevideo criteria and allow Liberland to gain the recognition it seeks." ROSSMAN, Gabriel, 2016, "Extremely Loud and Incredibly Close (But Still So Far): Assessing Liberland's Claim of Statehood", in *Chicago Journal of International Law*: Vol. 17: No. 1, Article 10. Available on line

[1572] In February 2023, Liberland opened its first international office (embassy) in Mexico. For more information, see "Grand Opening of the Liberland Office in Mexico City".

Appendix 5: Recognition and adoption of bitcoin as legal tender in El Salvador

In 2021, El Salvador became the first country in the world to recognize bitcoin as legal tender, via the adoption of the Bitcoin Law ("*Ley Bitcoin*") by the Salvadoran Parliament on June 9, 2021[1573] . The President of El Salvador, Nayib Bukele, had announced this intention on June 6, 2021, setting a precedent for the world of crypto-assets and especially for the Bitcoin blockchain ecosystem. This law gives bitcoin official status throughout the country, which has a population of almost 7 million[1574] . It's worth noting that while Liberland adopted bitcoin back in 2015, it is not an internationally recognized state, which therefore only relatively confers its place as the first state to legalize bitcoin in comparison to El Salvador[1575] . The law of June 9 obliges Salvadoran economic players to accept this virtual currency as a means of payment for their day-to-day transactions, marking an important turning point for the monetary facet of this asset. This is the first time that a constitutional state has officially recognized bitcoin as a currency, giving it legal tender status for the first time[1576] . The government is therefore obliged to provide the IT resources needed to implement this law, but bitcoin's limited technical infrastructure and price volatility are arousing both enthusiasm and concern among some local economic players, citizens and international financial institutions. In developed countries, citizens have access to a reliable and stable currency. However, this does not apply to the majority of the world's countries, as developing nations account for around 85% of the world's population[1577] . Indeed, the majority of these developing countries are not fortunate enough to have banking and financial systems as developed, stable and reliable as those in Western countries. This means that populations facing a lack of bancarization tend to perceive bitcoin as a more viable solution than their official currency, which often cannot be trusted due to unstable political regimes and/or monetary systems. As such, bitcoin particularly meets certain banking and financial needs for these countries[1578] , as is the case of El Salvador, which strongly supports this digital asset. In order to avoid common confusion surrounding the value attributed to bitcoin, this study distinguishes two of its main characteristics: bitcoin's ability to serve as a store of value, already recognized due to its adoption and rising price for over 14 years, and its function as a safe-haven asset, which is relevant in times when

[1573] "Ley Bitcoin | Asamblea Legislativa de El Salvador", June 9, 2021, available at.
[1574] HETZNER Christiaan, March 14, 2022, "El Salvador's millennial president launching Bitcoin 'volcano bond' in major bet on cryptocurrency craze", available at.
[1575] D'ANCONIA Frisco, November 16, 2016, "Free Republic of Liberland Values Bitcoin, But Ready to Move on to Dash," available at.
[1576] LAURANT Dominique, lawyer at the Paris Bar, October 21, 2021, "Puisque le bitcoin est la monnaie du Salvador, il faut en tirer les conséquences fiscales en France", "Manifestement, depuis le 7 septembre 2021, le bitcoin est la monnaie légale du Salvador. It therefore has the legal status of a currency in El Salvador, like the Swiss franc in Switzerland, or the rouble in Russia. It's hard to see how it could be said that bitcoin would not have 'the legal status of a currency'. Since that date, it is no longer a digital asset within the meaning of article L 54-10-1 of the CMF, and is therefore no longer covered by the tax provisions of article 150 VH bis of the CGI", available at the following address
[1577] Visit worlddata.com to see the list of 152 developing countries.
[1578] However, for the countries in question to be able to use bitcoin as an alternative currency on a large scale, it is essential that they have adequate Internet coverage enabling mass transactions.

of crisis, such as on the financial markets or in times of international geopolitical tension (Ukraine, etc.). On a more positive note, bitcoin seems to have enjoyed safe-haven status for only a few years now, a status that gold has acquired over the millennia.

El Salvador's stated political objective is to free itself from the traditional monetary and financial system by adopting a technology whose potential has so far been underestimated by certain Western institutions (IMF)[1579] . To achieve this goal, the country's population is to become as bankable as possible, by offering simplified and industrialized access to digital wallets (compatible with Bitcoin's L1 and L2). The Salvadorian government's wallet is called "*Chivo*"[1580] . Thanks to several communities that are gradually forming the population on the ground, bitcoin has thus become a means of payment widely adopted by part of the country's poor population[1581] . El Salvador's adoption of bitcoin stems from a specific economic rationale: to obtain an inexpensive, reliable and fast means of exchange, enabling the country's financial inclusion and economic growth to be strengthened. Like a national digital currency created from scratch, such as the cryptographic euro[1582] , El Salvador decided instead to take direct advantage of the qualities of the Bitcoin network for its various assets, such as its network effect, immutability and accessibility, which have already been studied. It should also be noted that the plans of the enigmatic and controversial President of El Salvador (see below) are not limited to this legal and financial recognition of Bitcoin. Indeed, he intends to make his country a
As part of its pioneering "*Bitcoin-nation*" strategy, the company is offering a billion-dollar government bond in bitcoins ("*volcano bonds*")[1583] . The proceeds of this bond issue, aimed at investors around the world, will support the construction of public infrastructure, such as the development of a bitcoin mining operation *directly* powered by the country's volcanoes (geothermal), or the construction of a "*Bitcoin city*"[1584] at the foot of the Conchagua volcano.

In practice, however, it seems that the adoption of bitcoin as a currency is paradoxically associated with widespread use of the Dollar. Indeed, providers of digital wallets that enable citizens to exchange bitcoins depend on partial or total access to Dollar-denominated accounts and systems (American companies specializing in bitcoin now offer

[1579] IMF, "IMF executive board concludes 2021 article IV consultation with El Salvador", in *Press release n°22/13,* 2022, free translation from English "They [IMF Executive Board] stressed the need for strict regulation and oversight of the new Chivo and Bitcoin ecosystem. They stressed that the use of Bitcoin poses significant risks to financial stability, financial integrity and consumer protection, as well as the associated contingent tax liabilities. They urged the authorities to reduce the scope of the Bitcoin Act by removing Bitcoin's legal tender status. Some directors also expressed concern about the risks involved in issuing bitcoin-backed bonds", available at
[1580] For more information, visit Shivowallet.com, 2021.
[1581] Five million Salvadorans have adopted bitcoin as a means of payment, according to Salvadoran President Nayib Bukele, May 3, 2022, "The World's Coolest Dictator" [Video], 1.52 out of 13.38 minutes, *Discover Bitcoin*. November 24, 2021, "Bitcoin adoption in El Salvador (Hot debrief)" [Video]. YouTube.
[1582] See *above*, II, Title 2, 2.4.
[1583] R, Rémy (2023b, January 23). "Bitcoin volcano bonds: El Salvador passes crypto-asset issuance law". Journal du Coin. Available at
[1584] BUKELE Nayib, President of El Salvador, May 10, 2022, "Bitcoin City is coming," [Tweet]

their own in El Salvador). This interdependence is thus necessary for economic agents to promote and use bitcoins, which may, paradoxically, limit its status as a cryptocurrency. It should also be pointed out that, although the current President of El Salvador was elected democratically, there seems to be a serious risk of political drift towards dictatorship in the coming years[1585] . This could lead opponents of Bitcoin to invoke the cliché that a dictatorial state would use the Bitcoin network to strengthen its power or even to launder public funds, which would be catastrophic for the image of this computer network, which has in fact been factually apolitical for 14 years. Ultimately, El Salvador and Liberland are both examples of novel social, economic, monetary and IT experiments, with uncertain legal and political effects. Although some consider these experiments to be utopian, it's important not to fall into the illusion that building an entirely 3.0 society, i.e. one built exclusively on crypto-assets, would be viable. The reality is likely to be more nuanced, and there will certainly be a coexistence or fusion between the well-established conventional 1.0 and 2.0 systems, with those of the third generation (3.0), or even the latest generations (4.0 or 5.0). Although El Salvador's initiative is perceived as a threat and a risk by players in the traditional[1586] system, it represents a formidable laboratory for social innovation for technophiles, and for this reason deserves to be supported. The structural choices made here will be closely scrutinized by the whole world in the years to come.

[1585] ARTE. 21 mars 2023, " Salvador : vivre sous Bukele " | *ARTE Reportage* [Vidéo]. YouTube
[1586] MAIRE Vincent, February 12, 2023, "Salvador: le FMI se méfie toujours du Bitcoin, mais semble adoucir légèrement son discours". *Cryptoast*. Available at

Appendix 6: Focus and analysis of blockchain mechanisms and consensus

The notion of consensus

The word consensus comes from the Latin "*consentio",* meaning agreement and unanimity about something. Today, consensus means direct or latent agreement between several people. Within blockchain technology and its multiple components, consensus refers to the algorithmic and organizational methods by which a blockchain and its actors agree on the validity of its history, i.e. the validity and order of its transaction blocks. Sometimes referred to as a "*consensus mechanism*", such an algorithm represents in concrete terms the governance or method by which a blockchain achieves consensus, i.e. getting machines to communicate in a harmonized way in relation to rules and information communicated online. In concrete terms, its aim is to ensure the reliability of the records and copies of blocks synchronized by each of its nodes.

Focus 1: The resilience and stability of Proof of Work (*PoW)* as a justification for its power consumption

In addition to the information provided in Appendix 6 (Focus 1), *Proof of* Work *(PoW)* is a system used by certain public blockchains to guarantee the validity and security of transactions, with Bitcoin being its origin[1587] . In computer science applied to blockchain technology, a Sybil attack is a computer attack in which an actor maneuvers numerous nodes pretending to be honest nodes (in reality malicious) in order to induce other nodes in the network identified as honest to accept invalid or false data. The aim of such an attack is therefore to constrain the behavior of honest nodes by deceiving or corrupting them. In this respect, the invention of the Nakamoto consensus algorithm by the Proof of Work, in homage to its creator, was among other things specifically designed to prevent Sybil attacks aimed at a decentralized peer-to-peer (P2P) network. Indeed, Proof of Work (PoW) resists Sybil attacks by censoring the actor attempting to multiply its identity in order to take control of the network. For over 14 years, the PoW has been the most proven mechanism as a source of truth for the blocks of a public blockchain like Bitcoin. In the early days of Bitcoin, Satoshi Nakamoto wanted any participant to be able to add a block to the sequence of previous blocks. However, choosing a user at random means opening up the network to individuals who can claim to be more numerous than they actually are. This is one of the reasons why Bitcoin uses the Proof of Work (PoW) mechanism: each validated block is the result of a unique piece of work, theoretically impossible to reproduce or falsify in a short space of time. PoW is a consensus mechanism in which each block is "*mined*" by a group of individuals who own machines.

[1587] In reality, the *proof-of-work* concept was first imagined and proposed in a paper in 1993 by computer scientists Moni Naor and Cynthia Dwork, then developed and formally named as such in 1997 in a paper published by Adam Back and finally later cited in Bitcoin's *White Paper* in 2009.

dedicated to the network. It therefore secures the Bitcoin network[1588] , while all the nodes on the network verify this Proof of Work at a later stage, as described in Appendix 3.

In other words, some computers now used exclusively for the Bitcoin blockchain incorporate ASIC (*Application-specific integrated circuit*) chips[1589] . An ASIC is a computerized device that uses microcircuits for the sole purpose of extracting bitcoins from its protocol (a process known as "*mining*"). These machines, hereinafter referred to as "ASICs", assemble a continuous puzzle of transactions, which is then automatically verified by other conventional computers (nodes running the Bitcoin Core software[1590]). These nodes then simply verify the accuracy of this cryptographic puzzle. This operating mechanism makes the Bitcoin blockchain extremely secure and resilient to any attempt to corrupt its blocks. In practical terms, the PoW requires voluntary, paid users ("*miners*") to objectively and quantifiably demonstrate that they have expended energy, thus eliminating those whose energy expenditure and work do not comply with certain conditions defined upstream by the Bitcoin community's developers. As a result, the cost of a Sybil attack is possible but prohibitive on this network (see following table). A malicious miner, in order to succeed in his attack, must consume a very large amount of energy to produce blocks in an attempt to deprive the blockchain of its legitimate transactions. When a malicious miner attempts an attack by producing invalid blocks, the latter consumes electricity unnecessarily and must pay the corresponding cost and price. In short, thanks to PoW, Sybil attacks cannot trick a Bitcoin node into accepting a false copy of the previous block history. Indeed, this node only needs a connection to an honest node to resist this attack, since Bitcoin's consensus is based on the principle of the largest proof-of-work that has been performed on the chain, thus guaranteeing that it is the legitimate copy of the expected blockchain.

In strictly computer terms, during the[1591] *mining* process, an ASIC-type machine receives, via conventional Internet protocols (TCP/IP), a problem and a mathematical calculation to be solved. Once the mathematical challenge has been received, the ASIC solves it locally using its computing power.

[1588] GRUNSPAN Cyril, PEREZ-MARCO Ricardo, "double spend races", freely translated from English, "The consensus protocol and security of the Bitcoin network rely on the process of bitcoin mining and transaction validation", in *arxiv.org*, 2022, available at p.5.

[1589] This is a type of microchip specially designed to perform a single task or a small set of tasks (calculations). ASICs are often used when a device or machine needs to perform a particular function with a high level of efficiency or speed. These circuits are generally designed to perform one task at a time, but very quickly, and are therefore often more efficient in performing their designated task than a conventional microprocessor whose use is general-purpose, i.e. multitasking. ASICs are more expensive to produce than conventional microprocessors. [1590] *Op. cit.* In early 2023, over 43,000 Bitcoin nodes were counted and estimated by Global Bitcoin Nodes (a figure that far exceeds the number of nodes in other blockchains) - in *Bitnodes*. Consult these statistics online in real time, and download the *Bitcoin Core* software to 'become' a *Bitcoin node* via your conventional computer, available at

[1591] See screenshot and explanations below. Source from the following video and interview with Guillaume Girard, Bitcoin expert at Galaxy Digital Mining on October 14, 2021. See also, "Blockheader Research-Rachel Rybarczyk" [Video] available on YouTube

calculation[1592] and then distributes it via P2P over an Internet connection, which may be minimal. Once distributed, it submits its solution for confirmation to the other ASICs and nodes in the network, which then audit it, i.e. check that the solved proof-of-work is correct. Once 51% unanimity has been reached with regard to the calculation and other necessary information[1593] , a block of transactions containing this proof of work is attached to the said chain. Consequently, even if an attacker exceeds 51% of the network's *computing power* ("*mining power*" or "*hashrate"*), he cannot modify the Bitcoin blockchain's history without expending at least the same amount of energy again as was used to create it. This is almost impossible in practice due to the large number - and geographical dispersion - of these ASICs, estimated at 2.9 million in August 2022[1594] . By the end of 2022, an attacker - state(s), corporation(s) - would need around 1.5 million ASICs to effectively attack Bitcoin. In financial terms, it would cost around $260,000 per hour of attack to corrupt the[1595] network, a computer attack which would paradoxically cause the attacker to lose the billions of dollars worth of ASICs at stake. It is therefore virtually impossible to allocate the necessary ASICs and related energy while operating one or more industrial mining sites of this size and capacity[1596] . It seems even less likely that the bitcoin community would notice and react accordingly. It becomes increasingly difficult to attack it over time, because if an entity had wanted to attack Bitcoin, it should have done so ten years ago. In conclusion, not only would it be impossible to carry out a 51% attack on the Bitcoin network due to the massive amount of ASICs and energy required, but, even if an actor were capable of doing so, there would be a strong financial deterrent to doing so.

In addition, the aim is to understand how a bitcoin transaction works on the Bitcoin blockchain (L1) and its native network[1597] : when a user requests a BTC transaction, it is first sent to a waiting list called the "*Mempool*"[1598] . The size of each block

[1592] These machines are designed and specifically optimized for this mining process, and can test several hundred billion combinations per second in an attempt to find a winning key (a *hash* beginning with a sequence of "0 "s and called a "*nonce"*, see illustration below) and its associated reward. This means that the more ASIC-type machines a person owns, the more capable he is of finding these combinations, and therefore the greater his total remuneration in bitcoins.
[1593] In the screenshot below, see the two green frames that represent in color the information ("*version, Query chain*", etc.) contained in each unique *hash* from a previous block.
[1594] VICE News, "The Future of Bitcoin Mining and the Environment", 2022 [Video] YouTube
[1595] MITCHELL, "Assuming a modest price of 6¢/kWh, for XP consumption of 3.05 kW, each machine would cost $0.183 per hour of operation (1,411,347 * $0.18 ~= $260,000 per attack hour. Furthermore, the attacker could mine (6 blocks per hour * 6.25 BTC per block * 51%) ~19,125 BTC per hour, equivalent to ~$573,750.", 2023, available online on Twitter.
[1596] Running 1.5 million ASICs, each of which consumes as much energy as 5 refrigerators, is a daunting and currently impossible task.
[1597] Satoshi Nakamoto explains how Bitcoin works as follows: "The steps involved in making the network work are as follows: 1. new transactions are broadcast to all nodes. 2. each node collects the new transactions in a block. 3. Each node tries to find a difficult proof-of-work for its block. 4. When a node finds a proof-of-work, it broadcasts the block to all nodes. 5. Nodes accept the block only if all the transactions it contains are valid and have not already been spent. 6. Nodes express their acceptance of the block by working to create the next block in the chain, using the hash of the accepted block as the previous hash.", *op. cit*. Bitcoin Whitepaper, p. 3.
[1598] View transaction blocks being validated in real time at the following address

being limited to around 2,000 transactions per block, this means that each ASIC will try to validate the transactions that will earn it the highest fees. This mechanism, similar to a digital auction, enables users to position their transactions more or less favorably in this Mempool: the higher the fee a user chooses to have his transaction validated by a *miner*, the greater the chance that his transaction will be selected to form part of the next block. Once a miner has found a winning *hash* (hereinafter "*nonce*" in the illustration), and if no cheating is spotted by the network nodes, then the transaction is almost instantaneously and effortlessly included in a block. The *miner* is rewarded with 6.25 bitcoins[1599] plus the fees for each transaction included in this block. This logic and these processes have been repeated tirelessly and uninterruptedly every 10 minutes for 14 years, earning Bitcoin the name "*Timechain*" in reference to its almost clockwork reliability.

In short, the *mining* activity secures the Bitcoin blockchain through the random drawing of a miner who will generate the next block. This draw cannot be faked, as each miner must expend electrical energy in order to take part in it, in the hope of winning the associated stake. Then, in a relatively short second stage, the blocks are validated and verified by the network nodes (an activity which, like the previous lottery, does not require the expenditure of a lot of electricity, since the miners have already carried out the validated draw amongst themselves). It can be concluded that the PoW mechanism is reliable, resilient and stable, and gives the open blockchains that use it optimum protection in terms of resilience, since it is based, according to several studies, on thermodynamics[1600] , the theory of

[1599] In 2008, the reward per block was *50 bitcoins every ten minutes*; this was automatically *halved* on November 28, 2012 (*25 bitcoins* issued every ten minutes); then halved again on July 9, 2016 (*12.5 bitcoins*) and again on May 11, 2020 (*6.25 bitcoins*). In May 2024, this same reward of *6.25 bitcoins* issued every ten minutes will automatically evolve to *~3.12 bitcoins* issued every ten minutes.
[1600] "Definition of thermodynamics", 2022, in *cnrtl.fr*, available at the following address

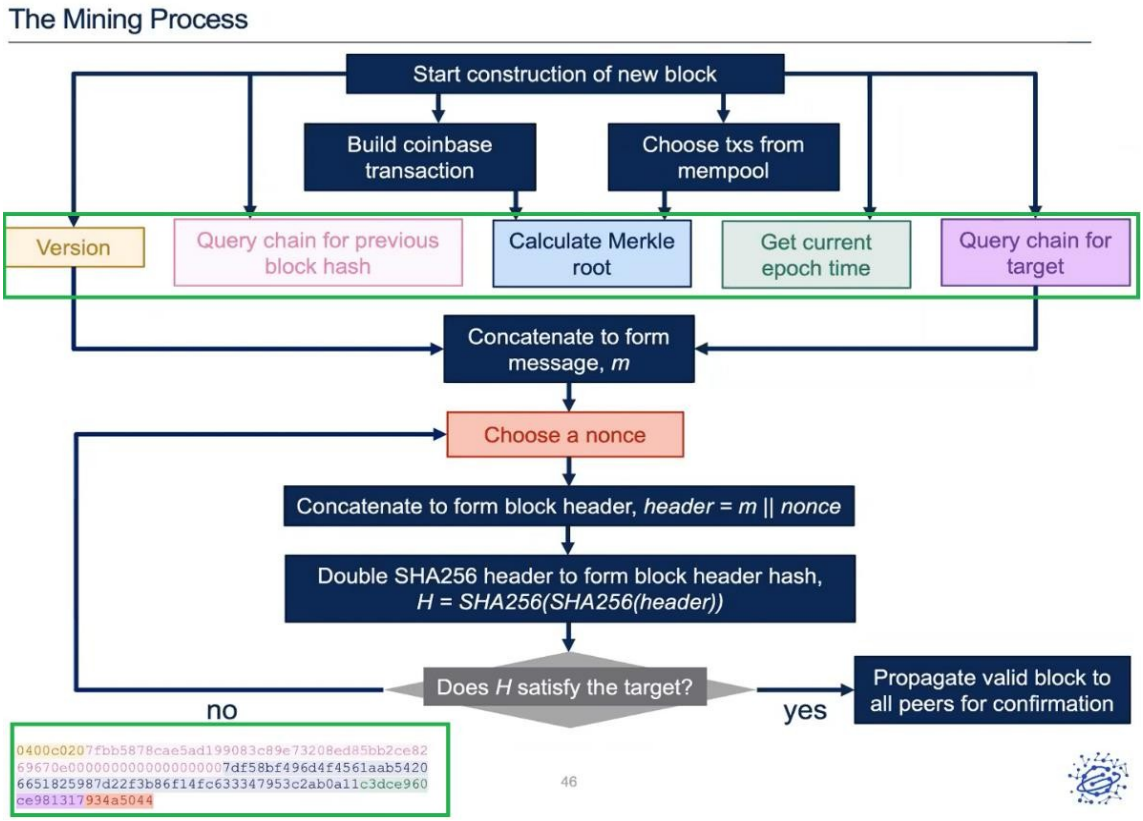
information[1601] , game theory[1602] and Darwin's theory of evolution[1603] . Finally, this novel computer consensus mechanism is sometimes referred to as part of a "*SoftWar*" movement[1604] , in reference to a peaceful software and social revolution. The following diagram illustrates the cryptographic and software layout and operation that make up part of the Proof-of-Work process performed by ASICs. To understand it in its most simplified form, we first need to observe that the two green frames. They correspond to the same sequences of information combined to form a *unique hash* or "*nonce*" (second green frame bottom left).

[1601] "Communications theory is concerned with the means of transmitting information from a source to a user", BELHADJ Besma, "Introduction à la théorie de l'information", 2011, p.1, available online.

[1602] Game theory. The Bitcoin protocol answers the "Byzantine Generals' Problem".

"Byzantine General's Problem", a game-theoretic mechanic. It was theorized in 1982 by Leslie Lamport, Robert Shostak and Marshall Pease and applied to the field of distributed computing. It states the difficulty faced by generals - some of whom may be traitors - who must reach a common agreement on whether to attack a city or retreat, but who can only communicate by sending messengers. The problem is to find a common strategy to ensure that the loyal generals can agree on a battle plan, despite the treachery of certain traitors who will retreat to thwart the attack. This problem is systematically solved (the attack will be a success) as soon as the traitors are in the minority and restricted. The purpose of this pictorial catachresis is to address some of the difficulties faced by distributed computers in communicating with each other (thanks to algorithms) in the knowledge that some of their peers (computers) are faulty, or even malicious. In other words, this synchronization challenge takes on its full meaning when applied to P2P networks of nodes wishing to agree on the contents of an electronic ledger: Bitcoin is based on a network of participants who each maintain the ledger of transactions carried out (the challenge is to agree on who owns what in a decentralized way, without relying on a central authority). Like traditional algorithms, the innovative "Nakamoto algorithm" used by Bitcoin enables a very large number of computers to participate in the transaction register in a totally open, decentralized way, without its operation suffering as a result. Finally, the Bitcoin protocol provides the first computerized solution to the "Byzantine Generals Problem", i.e. the problem of digital trust, without relying on a centralizing trusted third party and while preserving the pseudo-anonymity of its participants.

[1603] Free translation from English, "In this article, certain similarities between crypto-currencies and biological systems have been highlighted. [...] The analogy between Darwin's theory and evolutionary cryptofinance can be elaborated. A winning crypto-currency attracts capital because of a superior Sharpe ratio and other attractive protocol features. This is not a static but a dynamic problem, as developers try to gain an advantage by guiding t h e asset price and improving the protocol", BERNHARD K. Meister, C.W. PRICE Henry, "Darwin Among the Cryptocurrencies", Department of Physics & Centre for Complexity Science, Imperial College London, available online [1604] SCHRECKINGER Ben, "Space Force major to Pentagon: Mine Bitcoin!", in *Politico,* 2023, available at



Source: RYBARCZYK Rachel, in Galaxy Digital Mining, "Blockheader Research, 2022, YouTube

On the Bitcoin blockchain, each block consists of a "*header*" and a "*body"*, the latter itself being made up of multiple transactions. To create a valid block, a *miner* (ASIC) must *hash* this information using the SHA-256 algorithm to produce a new *hash* starting with a certain number of "0s" (here, for example, five zeros "00000e7042ac7d09c7bc41c8cfa5749e41858f6980643bc0db1a83cc793d3e24d3f77").

This greater or lesser number of 0s represents *the mining difficulty*. This is a statistical measure of the number of *hashes* that need to be generated to find a valid solution for solving the next block. By periodically adjusting the *difficulty of the network*, block issuance is maintained at an average of around 10 minutes between each block, which ultimately explains why a user has to wait at least ~10 minutes for a bitcoin transaction to be validated in a block.

This difficulty is determined by the number of 0s that must appear at the top of the output *hash* of a *miner*'s work. The more 0s there are in the output *hash*, the greater the difficulty, and conversely, the fewer 0s there are, the easier it is for a *miner* to find, i.e. calculate, the solution. Over time, the *difficulty of the network* increases, requiring *miners to be* constantly optimized to ensure profitability.

Since, as a reminder, each *hash* is unique and linked to an input datum, the part of the block that a miner modifies during the aforementioned mining/hashing process is called the "*nonce*" in red on the screenshot above. This is an exclusive, single-use sequence of numbers and "*bits*" used in a set of cryptographic operations). Thus, modifying this input, even slightly, radically changes the hashed output of the data set. A miner's job is thus to enter a *nonce*, *hash* it, then check his work until he finds the *winning nonce* (a *random*, but specific *nonce*, which enables the block to be validated thanks to the miner's work).

In other words, the miners quickly and randomly guess what this *nonce* must be. They *hash* it via the SHA-256 algorithm until they obtain an output with enough 0s to satisfy the ever-changing difficulty of the network (i.e. the fluctuating number of 0s required to find it). Finally, you can check this yourself on the mempool.space website: click on the number of a recent block, then count the number of 0s preceding its *hash*. This is how the whole network or any third party can know that it's a valid block, as the *hash* corresponds to the network difficulty at the moment of validation.

Having discussed the main foundations of Bitcoin in terms of its overall operation, it's important to address a crucial aspect of this technology and its future: its energy consumption. In this respect, it's important to make an essential distinction between energy consumption and power consumption. The notion of energy consumption is much broader than that of electricity consumption, which represents only one segment of the global energy market. Consequently, it is misleading to speak of the energy consumption of the Bitcoin network and it would seem more accurate to speak of its electricity consumption, unless the previous term "energy" is also used to include hardware and electronic waste such as the lifespan of the nodes and ASICs running on this network (which would complicate the scientific estimates studied in the table below). It is important to note that an analysis of the mining industry based solely on gross electricity consumption would be too narrow, as this industry has significant repercussions on the energy sector as a whole (both positive and negative). Indeed, the use of Proof of Work is particularly criticized for its energy-hungry nature, but it's also important to consider some of the compelling benefits it brings to the global energy grid. To illustrate this, the following table relates and notes two opposing arguments concerning the impacts of Proof of Work on the environment and consequently on society. It is rightly noted that former Member of Parliament Pierre Person underlined the complexity of this industry and warned certain institutional players against an overly simplistic analysis of this subject, which is in fact eminently strategic for Web 3.0[1605]
.

[1605] *Op. cit,* "Monnaies, banques et finance: vers une nouvelle ère crypto. Un enjeu de souveraineté et de compétitivité économique, financière et monétaire", "(...) to describe the mining industry in terms of its gross electricity consumption alone would be short-sighted in view of the complexity of an industry that involves significant impacts on the energy sector", p.70.

Arguments AGAINST Proof of Work	Arguments FOR Proof of Work
N°1: According to some studies and multiple more or less scientific articles, Bitcoin consumes excess energy (the equivalent of several countries combined)[1606] , i.e. around 0.6% of the world's energy produced[1607] . A 2022 study compares this figure to the 0.2% that is consumed by the conventional global payment system and agglomerated[1608] . As early as 2017, the World Economic Forum (WEF) estimated that Bitcoin would consume more energy than the entire world by 2020[1609] . In January 2022, another study estimated that the Bitcoin blockchain was responsible for around 19,000 deaths due to its energy impact[1610] . In May 2022, the Banque de France published and estimate in an economic review dedicated to blockchain that "*the energy consumption of a single Bitcoin transaction is equivalent to that of 834,000 bank card transactions* [...] *some protocols like Ethereum plan to abandon proof-of-work in favor of, in particular, proof-of-stake*	**N°1':** First of all, it should be stressed that every action undertaken by human beings requires energy, and that a growing society is necessarily an energy-consuming society. Society's tolerance of the pollution generated by this energy consumption is directly proportional to the utility and social necessity of the activity in question. In other words, the environmental consequences of a technology are more readily accepted if the benefits it brings are considered necessary by society[1612] **.** Understanding of Bitcoin's present and future benefits[1613] and, more broadly, of its role in society, is still limited and underestimated by a large proportion of economic agents due to its relative youth. The assertion that Bitcoin would consume all the world's resources by 2020, put forward by the World Economic Forum (WEF), is false and reflects a deliberate misunderstanding or misinformation, as evidenced by a video posted on the WEF's Twitter account in 2022[1614] . With regard to concerns the study linking the functioning of

[1606] HUANG, J. O'NEILL, C. & TABUCHI, H, "Bitcoin Uses More Electricity Than Many Countries. How Is That Possible? "2022, in *The New York Times,* available at

[1607] AGUR I. DEODORO J. LAVAYSSIERE X. MARTINEZ PERIA S. et al, "Digital Currencies and Energy Consumptions", 2022, in *Fintech Notes,* "As of April 25, 2022, the annual power consumption of the Bitcoin network is estimated at 144 terawatt-hours (TWh) per year according to the Cambridge Bitcoin Power Consumption Index. This represents around 0.6% of total global electricity consumption", p.9.

[1608] *Ibid.* "Overall, aggregating these estimates based on the parts of the payment system for which energy consumption data are available, we obtain an estimate of 47.3 TWh of annual energy consumption by the global payment system. This represents around 0.2% of total worldwide electricity consumption.
", p.27.

[1609] JEZARD Adam, "In 2020 Bitcoin will consume more power than the world does today", 2017, in *World Economic Forum (WEF),* accessed April 28, 2022, at.

[1610] TRUBY Jon, DEAN BROWN Rafael, et al., "Blockchain, climate damage, and death: Policy interventions to reduce the carbon emissions, mortality, and net-zero implications of non-fungible tokens and Bitcoin", Energy Research & Social Science, Volume 88, 2022, available online, translated from English "[...] many popular types of blockchain have resisted pressure to reduce their environmental impact, including bitcoin, whose annual emissions attributed to 2021 will produce emissions responsible for approximately 19,000 future deaths.".

[1612] For example, aviation or nuclear power are socially justified (like Bitcoin and without giving this disruptive technology a chance), see European Parliament, "Parliament rejects proposal opposing inclusion of nuclear and gas activities in list of environmentally sustainable activities", 2022, "Taxonomy: Parliament does not oppose inclusion of gas and nuclear activities", available online.

[1613] As a reminder, we refer to the benefits of Bitcoin listed here: fast, borderless transactions, a safe-haven asset, promoting financial, entrepreneurial and communication freedom, IT resilience and digital and political independence.

[1614] WEF, "A change in the way bitcoin is coded could almost eliminate its environmental impact," Twitter, accessed April 28, 2022, at.

(" à 99,95% less proofofstake")"[1611] .	Bitcoin at 19,000 deaths, our observation shows that this type of scientific reasoning is decontextualized and loses its interest, thus hindering an objective understanding of the issues linked to this new computing paradigm. According to the Banque de France review, which states that one bitcoin transaction is equivalent to 834,000 bank card transactions, this assertion cannot be verified or considered valid according to computer science, as it has no verifiable source. Similarly, the figure put forward in favour of "*Proof of Stake",* which would be less energy-consuming than "Proof of Work", is based on a purely theoretical assertion at the time of publication of this review. It seems that these figures and conclusions are motivated by a desire for strategic and political communication rather than scientific accuracy and neutrality. This stance is still widely held by some institutional players in the sector to hinder the general public's understanding and adoption of bitcoin. To illustrate this point, Greenpeace, an international organization that fights to protect the environment, recently launched a campaign in the USA to oppose bitcoin mining[1615] . Artist and activist Benjamin Von Wong was commissioned by Greenpeace to create a work of art to encourage public opinion to change Bitcoin's consensus mechanism from PoW to PoS. After creating the work and communicating about it online, the artist realized that the anti-Bitcoin campaign was unjustified. He therefore publicly admitted his mistake and changed his opinion on the subject, now supporting the potential of the Bitcoin network to serve the energy transition[1616] .

[1611] V. Focus 2 of this Appendix, *see* also "ABC l'éco en bref, la blockchain", Banque de France and EDUCFI, p.3, available online at

[1615] CANTON Ben, "'Change the code, not the climate' Greenpeace launches new assault on Bitcoin", March 30, 2023, in *Journal du Coin,* available at the following address

[1616] Free English translation, "The #SkullofSatoshi is a phenomenal accident. It literally represents what both sides believe to be true: that Bitcoin has the potential to be more environmentally friendly; a positive force for the environment.", "The SkullofSatoshi is a phenomenal accident," March 25, 2023 on Twitter.

	In July 2021, the "*Bitcoin Mining Council - BMC*"[1617] conducted a survey of over 32% of the global Bitcoin network, the results of which revealed that almost 67% of miners use electricity ("*energy mix*")[1618] from sustainable sources. On this basis, and given the network's expansion, it is possible that mining will become one of the most efficient and sustainable industries in the world, as also highlighted in a report by the French National Assembly in 2022[1619] . According to the BMC, Bitcoin would actually consume 0.17% of the world's energy produced as of January 2023[1620] . In January 2023, an article published in the MIT Technology Review highlighted some of the direct benefits of Bitcoin mining in the Congo, where Virunga National Park became the first national park to operate a Bitcoin mine in order to protect its forests and famous wildlife[1621] .
N°2: Bitcoin has limited or no social value or utility, which means it has little or no use in our society, except for financial speculation.	**N°1' & 2':** Methods, basis of calculations[1622] and comparison used to denounce the supposed *The claims that* the Bitcoin network is an "*energy waster*" are gradually being refuted[1623] as more and more is understood about its hardware and structure, as well as its software. In other words, the more Bitcoin is studied and understood, the more its energy-guzzling nature will be nuanced, if not socially justified (see below).
No. 3: Bitcoin has little or no economic value. The banking system and conventional finance is more efficient and	**N°1' & 3' & 4':** According to a study published in April 2022, to refute the assertion that "*the*

[1617] Bitcoin Mining Council, "Bitcoin Mining Council Survey Confirms Sustainable Power Mix (Q2 2021)". bitcoinminingcouncil.com

[1618] Wikipedia contributors, "Energy mix", accessed April 1, 2022, at

[1619] "While bitcoin mining does indeed consume a lot of energy, sometimes carbon-based electricity, it can also be a particularly effective activity for financing the ecological transition.", *op. cit.* "Currencies, banks and finance: towards a new crypto era. A challenge for sovereignty and economic, financial and monetary competitiveness", p.72.

[1620] Bitcoin Mining Council, "Bitcoin Mining Council Q4 2022 Briefing," [Video]. YouTube.

[1621] POPESCU Adam, "Gorillas, militias, and Bitcoin: Why Congo's most famous national park is betting big on crypto," 2023, in *MIT Technology Review,* "In a bid to protect its forests and famous wildlife, Virunga has become the first national park to mine bitcoin," article available at.

[1622] According to the *Digiconomist* blog (initially used as a source for the proposed amendment and ban on Bitcoin mining for the MiCA regulation), whose basic calculations from their *Bitcoin Energy Consumption Index* are scientifically false and biased, the Bitcoin network would consume the equivalent of 42.6% of the electricity produced in France in 2022. These biased calculations are explained by the fact that (i) miners are located by country according to their IP addresses, even though many use *VPNs* (the data is therefore biased from the outset), (ii) the *energy mix of* the country in question is applied to the miners (without taking into account the real, unique and effective consumption of each miner's installation). "Bitcoin Energy Consumption Index - Digiconomist, 2022, in *Digiconomist.* Available online

[1623] STACHTCHENKO Alexandre, "[...] most of these load-bearing studies have absolutely no understanding of how Bitcoin works or what it replaces", 2022, "Manuel de survie dans la jungle des poncifs anti-Bitcoin (version longue)", in *Medium*, accessed on April 1, 2022 at.

reliable than the decentralized system proposed by Bitcoin. **N°4:** If Bitcoin were to be widely adopted with millions more users, it will face problems of bugs, network congestion and high fees, demonstrating its long-term unsustainability.	*Cryptocurrencies are worthless*"[1624] , it is relevant to compare the performance of traditional payment systems with that of the Bitcoin protocol. According to the study, a Bitcoin transaction is on average 288 times faster than a conventional payment transaction[1625] , while Bitcoin consumes 56 times less energy than the traditional system[1626] . Furthermore, the study suggests that Bitcoin is not fully exploited, as it is possible to increase transaction volumes by up to four times without increasing its energy consumption, even on its L1, without even taking into account the existence of L2s such as the Lightning Network. Finally, the author of the study points out that even at the level of a single transaction, a PoW transaction proves to be 1 to 5 times more energy-efficient[1627] . It should be noted that, according to the author, the study's margin of error is 4%, and that the figures intentionally underestimate the results[1628] . **N°1' & 2' & 3':** To be profitable, the business model of bitcoin miners relies on reducing electricity costs, while bitcoin revenues must cover these costs[1629] . However, fluctuations in the bitcoin price are uncontrollable for miners, who must adapt their behavior accordingly. Miners are geographically mobile and independent, as they move from country to country[1630] to find low-cost energy sources, including subsidized renewables[1631] . They can do this regardless of infrastructure and

[1624] KARAYAN, Raphaële, "Les cryptomonnaies ne valent rien selon Christine Lagarde", 2022, in *usine-digitale.fr*, accessed June 9, 2022, at.

[1625] KHAZZAKA Michel, "Bitcoin: Cryptopayments Energy Efficiency", 2022, p.1, available at "A conventional payment transaction is on average 288 times slower than a bitcoin transaction".

[1626] Grand Angle Crypto, "A war of communication!" [Michel Khazzaka], 2022, [Video]. YouTube, "Bitcoin consumes 56 times less energy than the classic system".

[1627] *Op. cit,* "Bitcoin: Cryptopayments Energy Efficiency", 2022, p.1, available online at, "We show that (...) even at the level of a single transaction, a PoW transaction turns out to be 1 to 5 times more energy efficient."

[1628] "A war of communication!" [Michel Khazzaka], July 6, 2022, [Video], YouTube.

[1629] *Op. cit,* "Monnaies, banques et finance: vers une nouvelle ère crypto Un enjeu de souveraineté et de compétitivité économique, financière et Monétaire", "miners tend to seek the lowest electricity prices", p.70.

[1630] *Ibid.* "As mining farms were extremely mobile, miners could afford to shift their activities according to energy costs and thus consume more without suffering a substantial increase in their production costs", p.69.

[1631] Hydroelectric, geothermal, solar or wind power plants, etc. For more information on bitcoin mining from geothermal energy, *see* the following video by Grand Angle Crypto, 2022, "Mining Bitcoin in El Salvador? .... .let's get serious!" [Video]. YouTube.

	existing resources, as only electricity and a minimal Internet connection are required to mine bitcoins. Currently, low-cost energy is found in isolated areas with low energy demand, such as Siberia[1632] , some African countries and Kazakhstan[1633] , where the electricity produced is wasted due to lack of use. Miners therefore propose to use this wasted energy to support a universal, independent and resilient financial infrastructure such as Bitcoin. Since 2020, green *mining* initiatives have been multiplying, such as the use of certain polluting materials wasted by the oil industry in the USA[1634] or animal waste from farms in Ireland[1635] . **N°4':** The Lightning Network (L2) offers the possibility of carrying out low-value transactions without requiring the use of Bitcoin's native blockchain (L1)[1636] , thus reducing congestion and costs on this main L1 network. With the arrival of new users, it is conceivable that they will gradually be redirected to the L2, specially designed for low-value, optimized payments. In this respect, one of the US Federal Reserve's (FED) bodies recognized in 2022 that the Lightning Network is a significant step forward for bitcoin as a credible payment network[1637] , due to its ability to offer scalability and efficiency far superior to those of the payment system conventional (traditional finance), and by being

[1632] CHULAIN Aisling Ni, "How this Siberian data center is attracting Bitcoin miners with cheap, 'green' power", 2021, Euronews, accessed April 1, 2022, at.

[1633] ARNOULT Maxime, "Kazakhstan attracts bitcoin producers from all over the world, here's why", 2022, in *ouest- france*. Retrieved April 1, 2022, from

[1634] For more information see the following video from Forbes Digital Assets, December 20, 2021, "Mining Bitcoin With Natural Gas For A Clean Crypto Future," in *Business of Climate Change Forbes*, [Video]. YouTube.

[1635] For more information see the following video from Cointelegraph, 2023, "How Irish farmers are turning cow poop into digital gold (Bitcoin)". YouTube.

[1636] AGUR I. DEODORO J. LAVAYSSIERE X. MARTINEZ PERIA S. et al, "Digital Currencies and Energy Consumptions", 2022, in *Fintech Notes,* "Substitution effect: for a given level of demand for asset transactions, Layer 2 [Lightning Network] reduces demand for on-chain [L1] transactions by allowing more off-chain transactions, which reduces transaction fees (transaction fees depend on transaction demand) and the incentive to mine, which would in turn reduce energy consumption.", p.12.

[1637] ZIMMERMAN Peter, DIVAKARUNI Anantha, "The Lightning Network: Turning Bitcoin into Money", "Our results suggest that the Lightning Network can help Bitcoin achieve greater scalability, enabling it to function better as a payment system. According to our results, if the LN had existed in 2017, congestion [on the main Bitcoin network (L1)] could have been 93% lower.", p.3, available at

	up to a million times more energy-efficient per transaction than instant payments[1638] .
N°5: China's mining ban in 2021[1639] demonstrates not only that the PoW mechanism is economically and ecologically unsustainable in the long term, but also that central bank digital currencies (CBDCs) are the way forward.	**N°2' & 3' & 5':** The Lightning Network already enables certain IT mechanisms (other than IND) that allow users to authenticate themselves on online financial services[1640] . These new 3.0 initiatives, built on and linked to the LN, are multiplying, echoing and appealing to the INAS concept. Just as the banking sector has had to develop its own identification mechanisms, the Bitcoin ecosystem seems to be successfully building its own. In this respect, and as a reminder, the identification and authentication mechanisms required to implement an MNBC are also being developed on Bitcoin, but with other 3.0 IT standards. **N°5':** The final effect of China's mining ban was the relocation of thousands of ASICs to the USA (Texas), Canada and Kazakhstan. As a result, the majority of these machines are now back in operation, securing the Bitcoin network, which reached an unprecedented level of computing power just a few months after the Chinese ban[1641] . The political and economic aim of this ban is to support the gradual launch of digital Yan throughout China. In France, some researchers are also proposing to ban PoW and the pseudo-anonymity associated with it. system[1642] , in particular to promote

[1638] *Ibid.* "Bitcoin: Cryptopayments Energy Efficiency", p.1, available online at, "When the Bitcoin Lightning layer is compared to the [conventional] instant payment system, Bitcoin gains exponentially in scalability and efficiency, proving to be up to a million times more energy efficient per transaction than instant payments.".

[1639] China considered banning bitcoin mining as early as 2019, but it wasn't until 2021 that the authorities imposed severe restrictions on players in this industry. In 2021, the *mining* ban finally prompted companies to leave the country and turn to countries like Kazakhstan, which have a more favorable stance towards the industry. They have also found refuge in cities in the United States, where companies encounter both support and criticism from the local population and politicians. To understand how China has positioned itself since 2013 in relation to crypto-assets and Bitcoin in particular, V. the following article "All You Need to Know About China #39; s Crypto Ban.", 2022.

[1640] For example, reference is made to the "*LNURL"* communication protocol between Lightning wallets and external applications or third-party services. The French company *LNMarkets* uses "*LNURL-auth*" for the connection: the user's wallet derives a new key pair that is linked to the company's services. The node's public key is therefore masked from the latter, and the apparent public key used for connection will be different when accessing each service.

[1641] These statements are verifiable thanks to multiple analyses of objective data, available at "Bitcoin Hashrate Chart", in *BitInfoCharts.*

[1642] DELAHAYE Jean-Paul, "Logique & Calcul : Des crypto-monnaies sobres en énergie ?", in *Pour la science N° 536* / Juin 2022, "Despite the admiration we owe to Satoshi Nakamoto, the inventor of the first cryptocurrency, Bitcoin, his

	private and hybrid blockchains, and probably to support the forthcoming launch of a dispensable crypto euro. Given these facts, it seems that a total ban on bitcoin mining is utopian because of its anti-fragile nature, i.e. it is designed to bypass all censorship.

Conclusion and outlook

- To sum up and complement the above data, Bitcoin's environmental impact varies considerably depending on the country where it is mined. In some countries, electricity is produced mainly from renewable energy sources, which may reduce Bitcoin's overall environmental impact. In other countries (China), where electricity was generated from non-renewable energy sources, its environmental impact no longer seemed socially and ecologically justifiable.

- It is currently difficult to determine to what extent data from the traditional financial system can be compared with that from the Bitcoin network due to biases
  We are also aware of the risks of political misinformation on the part of stakeholders involved in the studies carried out and mentioned. Indeed, every calculation method used is open to interpretation. Consequently, only a long-term analysis will provide a scientific and objective answer to the question of whether Bitcoin is really dangerous for society and contrary to the current drive to combat global warming. To do this, it would be necessary to draw up a list of objective criteria, widely recognized by the scientific community, to enable valid comparisons. The purpose of this table is precisely to provide a trace of the data and positions relating to the Proof of Work, concerning the period 2020-2023, to facilitate subsequent updating by other researchers.

- Until now, the job of *miners* was mainly to stabilize the power grid, rather than to waste electricity[1643] . In fact, their role was to absorb excess of electricity produced by traditional energy infrastructures[1644] , which was often wasted, as it was difficult to store or transport. By making up for this under-utilization of the electricity grids of certain countries, *miners* have made it possible to finance the development of these infrastructures, in particular towards renewable energies, by selling part of the bitcoins they have mined. It should be noted that *miners are* above all looking for profitability. economically, i.e. by seeking to extract bitcoins at a cost lower than that of the

Proof of work' is undoubtedly an absurdity. It must be abandoned if we really want this new kind of currency to develop, enabling the existence of anonymous digital cash that respects everyone's privacy [cryptographic euro]".

[1643] SANSFACON Jean-Robert, "Cryptomonnaies: pour qui l'électricité?", "À Québec, le gouvernement Couillard est partagé entre la crainte d'être envahi par ces gaspilleurs d'énergie qui facilitent la vie du crime organisé et le risque de rater le coche des technologies de l'avenir.", 2018, in *Le Devoir*, available at.

[1644] PERSON Pierre, Rapport de l'Assemblée nationale, *op. cit,* "As production is difficult to anticipate, it regularly leads to large surpluses when distribution 75/204 networks are not sufficiently dimensioned. Thus, the poor distribution of distribution networks and the inability of the renewable sector to store the electricity produced is a godsend for bitcoin miners, who can buy energy at low cost. This is a reciprocal windfall between producers and consumers, as this energy would not have found a buyer [without bitcoin miners]", p.74.

international market[1645] . In the past, governments subsidized fossil fuels, which had the effect of reducing the cost of electricity generated from these sources. In this context, miners were tempted to use these carbon-based energy sources for their activities, which nevertheless accounted for only 33% of the electricity consumed by the grid in 2021. By 2023, subsidized energies appear to be mainly renewable, gradually encouraging *miners* to turn to these new sources of energy at decreasing cost[1646] . It is important to stress that only *miners* using green energy sources will eventually be allowed in developed countries, given the growing awareness of climate issues. It's also time to put an end to the preconceived notion that "*wild mining", i*.e. mining using irregular energy sources (undeclared, stolen and carbon-based), still accounts for the majority of this Web 3.0 industry. It should be remembered that, in addition to its increasingly obvious social and economic usefulness, Bitcoin's economic incentive and computing mechanism are helping to innovate towards an energy transition and new, more sustainable and less costly sources of energy[1647] . Consequently, a legal ban on PoW would be counterproductive from both a scientific and a social point of view. Society needs to get to grips with the subject in order to collectively judge the extent to which Proof of Work can be accepted in certain activities and sectors. This is all the more necessary for the future of the ecosystem, which could not survive in the long term without it.

- In short, *miners* are looking for low electricity costs and politically stable countries for their mining activities, and many miners have, for example, settled in
in Texas to escape the ban on their activities in China[1648] . A White House report published in August 2022 acknowledges for the first time that these activities can make a positive contribution to the energy transition[1649] . A survey conducted in May 2022 by Forbes newspaper also estimates that over 80% of Americans do not believe that bitcoin-related investments threaten the environment[1650] . In France and the EU, on the other hand, the situation is different, and there is a need for *ad-hoc* legislation - partly binding, but also attractive - to encourage the greenest *miners* to set up shop in Europe. This would encourage job creation in this booming industrial sector, with its high added value for the entire European blockchain ecosystem,
which could also benefit the private and hybrid blockchains studied. It is

[1645] For example, on January 9, 2023, the average cost of mining a bitcoin for a miner is $13,000, while its average exchange value is $16,000. This difference of $3,000 at this time *t* means that it's still profitable to *mine* for these *miners*, who earn the $3,000 from this price difference. Prices and data taken from the following site, in *TheMinerMag*,
"Estimated Cost of Bitcoin Production".
[1646] For example, the operators of the Texas National Grid ("ERCOT") use bitcoin miners to help stabilize the state's fast-growing renewable energy infrastructure, particularly during periods of high electricity demand (during peak periods, *miners* cease operations and vice versa), CONNELL Shaun, CARTER Nic, "Miners Are The Optimal Buyers: The Data Behind Bitcoin-Led Decarbonization In Texas.
"in *Bitcoin Magazine*, 2021, available at
[1647] *Ibid.* Report for the French National Assembly, "Bitcoin miners seem to be moving naturally towards renewable energy sources", p.74.
[1648] Motherboard, "How Bitcoin Mines Were Airlifted From China to the US," in *CRYPTOLAND* Episode 7, (April 21, 2022) [Video]. YouTube.
[1649] Translated from English "[...] crypto-asset mining operations that capture vented methane to generate electricity may have positive climate outcomes, converting the potent methane to CO2 during combustion. Mining operations, however, may be more reliable and efficient at converting methane to CO2.", The White House, "Climate and energy implications of crypto-assets in the united states", 2022, in *whitehouse.gov*. Retrieved September 9, 2022, from p.24.
[1650] DUGGAN Wayne, "Survey: 84% of Americans don't believe that Bitcoin investments are a threat to the environment", 2022, in *Forbes Advisor*. Available at

The European Union could set up a dedicated *regulatory sandbox* to test new financial services or business models under real-life conditions. The proposals put forward by former MP Pierre Person in his report to the French National Assembly[1651] should be carefully examined. They include promoting partnerships between energy producers and crypto-asset miners, as well as banning the mining of crypto-assets from carbon-based energy sources, by adjusting the regulations applicable to pollution rights[1652] .

- As explained and assumed above, bitcoin mining could progressively finance the development of clean energies, an opportunity that is starting to take off.
be recognized by certain companies[1653] and even by some of the institutions mentioned. The latter see mining as essential to stabilizing and decarbonizing the electricity grid and its currently under-utilized infrastructure, as in Texas[1654] and El Salvador mentioned above. In August 2022[1655] , 2% of Texas' electrical power was allocated to bitcoin mining, a figure whose positive or negative interpretation depends intimately on each observer's perception of the social utility of this monetary and financial network. Ultimately, only the education of the political body[1656] and lobbying could ultimately forge partial or total social acceptance, which will probably form the basis for subsequent litigation (thus creating a body of case law). Bitcoin is a system that offers a fixed price for energy, as it enables us to put a theoretical price on large quantities of renewable energies that are currently being used in a sub-optimal way. In the end, it's all about staying in touch with the reality on the ground on a subject as technical as it is transversal, so that ecology remains connected to reality and doesn't become an ideological weapon in the service of ideals biased by continuous political and/or institutional disinformation.

- In the light of the above information, Bitcoin mining presents an *energy mix of*
of around 60% from renewable energies, which means it looks 'greener' than what
than even the most reluctant of institutions might allow. Over the next few years, and according to a statement issued in 2022 by the European Commission, the latter is looking to "*promote 'environmentally friendly' consensus mechanisms through the European Blockchain Services Infrastructure* [EBSI] *as the gold standard in Europe and worldwide,*" including by developing "*an energy efficiency label for blockchains.*"[1657] , as well as publishing a report by 2025 "*that will include a description of the environmental and climate impact of new technologies on the crypto-asset market. The report will also include a*
assessment of policy options for mitigating the negative climate impact of

[1651] *Op. cit,* PERSON Pierre, Rapport de l'Assemblée nationale, "Faced with the ban called for by some, this report defends the view that public authorities should implement a policy to steer miners towards clean energies and reward those who finance the ecological transition", p.78.
[1652] ACPR. "A Regulatory Sandbox. Une Sandbox réglementaire - bac à sable réglementaire - pour quoi faire?", 2019, p.1, available at.
[1653] Blockstream, "Blockstream and Block Inc.'; s Solar Mining Facility, Now Powered by Tesla Solar PV and Megapack," 2022. Retrieved June 1, 2022, from
[1654] WEBB Shelby "Texas renewables generated record power in early 2022", 2022, in *Houston Chronicle*, accessed May 3, 2022, at
[1655] VICE News, "The Future of Bitcoin Mining and the Environment," 2022, [Video]. YouTube
[1656] Sénat, hearing "Regulation and innovation in the field of cryptoactives", round table, Faustine Fleuret's intervention, in *videos.senat.fr*, (viewing at 12:15).
[1657] Communication: Digitizing the energy system - EU action plan, COM(2022)552/2, accessed on October 18, 2022, at p.17.

technologies used in the crypto-asset market, particularly with regard to consensus mechanisms". While these decisions are necessary and seem coherent in light of the energy crisis in 2023, it is argued that the current political motivation against the PoW mechanism is only partially justified and poses a systemic risk to the European blockchain and technology ecosystem. It is emphasized that this political will seems not just European, but international: "*As Europe currently only accounts for around 10% of proof-of-work mining* [actually more like 1.5-2% according to other experts][1658] *, international cooperation is needed to tackle the high energy consumption of proof-of-work mining in a way that has a global impact.*"[1659] .

- It's important to be pragmatic when it comes to bitcoin miners, because only *miners* using low-cost, low-carbon electricity sources (known as "*mining*
  In the long term, the "*sustainable*" or "*green mining" companies will be* able to survive ("*the survivors"*)[1660] . These are the only profitable and socially accepted activities, as other *miners* using carbon-based electricity sources such as coal or oil will gradually disappear due to insufficient social and political support to sustain their activities. In March 2023, a unique bitcoin mining experiment, Nautilus, was launched in northeastern Pennsylvania. This *mining facility* is set up by the Terawulf company and, for the first time in the world, uses a nuclear energy source[1661] ,
  This is a revolutionary idea, even though it was unthinkable just a few years ago: "*sustainable*" as defined by the European Commission .[1662]

- According to a prospective study published in August 2022[1663] , it is possible that Bitcoin's energy consumption will increase considerably if its price reaches $2 million in
  2040 (a fantasy estimate today, but not to be underestimated in the longer term). According to this study, Bitcoin's electricity consumption could increase by a factor of around 10, from 0.05% of the world's electricity in 2022 to 0.36% in 2040. However, other studies estimate this figure at 0.55% in 2021[1664] and 0.6% in 2022 respectively (*see* the study cited in argument N°1 of this table). Bitcoin's energy consumption therefore depends on its price, and if it reaches $500,000 in 2040, its consumption could exceed 0.1% of the world's electricity, a more plausible figure at this stage. Although Bitcoin's future energy consumption is uncertain and depends on a number of factors, the author of the study considers that bitcoin mining will be considered
  as an energy-intensive industry[1665] , but would remain well below

[1658] STACHTCHENKO Alexandre, Twitter. 2022, available at
[1659] Communication: Digitizing the energy system - EU action plan, *op. cit.* p.17. [1660] Grand Angle Crypto, "The theory of the last survivor in crypto mining!", 2022. [Video]. YouTube [1661] Terawulf, accessed February 16, 2023, *v.* "Nautilus Cryptomine" project. Available at
[1662] Proposition de résolution au nom de la commission des affaires européennes, en application de l'article 73 quater du Règlement, sur l'inclusion du nucléaire dans le volet climatique de la taxonomie européenne des investissements durables: L'inclusion de l'énergie nucléaire dans la taxonomie européenne des activités durables, in *sénat.fr*, 2021, available at the following address
[1663] MELLERUD Jaran, "How much energy will Bitcoin consume in the future?", 2022, in *Arcane Research*. Available online
[1664] CARTER Nic, "According to the Cambridge Center for Alternative Finance, bitcoin currently consumes about 110 terawatt-hours per year, or 0.55% of the world's electricity production, or the equivalent of the annual energy consumption of small countries like Malaysia or Sweden," "How Much Energy Does Bitcoin Actually Consume?", 2021, in *Harvard Business Review*. Available at
[1665] *Ibid.* What determines Bitcoin's future energy consumption? 1) The price of BTC 2) Transaction fees 3) The percentage of miners' income spent on energy 4) The average energy price of Bitcoin miners",

sectors such as cement production, which will already consume more than 2% of the world's energy by 2022[1666] .

- Ultimately, the key focus of this Annex is whether spending between 0.17%, or a maximum of 1% of the world's electricity in the long term, to recall electricity optimized and renewable energy through mining, in order to secure a financial infrastructure accessible to billions of people, will be socially beneficial and justified for and by society. Although the figures are relatively uncertain at this stage, this question needs to be closely examined by each and every one of us. According to Daniel Batten, investor, author and specialist in new climate-affecting technologies, the first clue is that Bitcoin is quite simply a "*counter-intuitive solution*" in the fight against climate change[1667] . In other words, this system is unfairly discredited due to a lack of knowledge about it, even though it could represent a crucial system for achieving certain international climate objectives.

Focus 2: *Proof of Stake (PoS*) as a supposed alternative to PoW

Proof of Stake (*PoS) is* another consensus mechanism introduced in 2012[1668] . This alternative consensus mechanism was designed along the same lines as the Proof of Stake mechanism described above. Proof of Stake delegates network validation and control to the owners of the network tokens. In other words, it assigns responsibility for block validation to users according to their financial stake in the blockchain. More specifically, users who own tokens on the said blockchain can

In practice, validator nodes deposit and "*stake*" the tokens they hold on a specific smart contract. In practice, validator nodes deposit and "*stake"* the tokens they hold on a specific[1669] smart contract. In this way, the escrow acts as a (crypto)financial guarantee. If they disregard the network rules or make fraudulent decisions (attempt to corrupt blocks and the network), said users and validators are automatically penalized by the algorithm, i.e. deprived of all or part of their initially escrowed tokens. In this sense, this escrow is sometimes presented as a theoretical improvement over the PoW mechanism, as it requires neither specialized hardware (ASIC) nor significant power consumption (the PoS energy footprint is therefore smaller, transaction validation time shorter, transaction volumes higher, but overall IT resilience weaker). While several blockchains have attempted to implement

[1666] Words freely translated from English and taken from an excerpt published by Jaran Mellerud on his Twitter account, August 23, 2022, "With such high energy consumption, bitcoin mining will be considered an energy-intensive industry, but still a far cry from industries like cement production, which consumes 2% of the world's energy."
[1667] BATTEN Daniel, "Bitcoin Mining Can Prevent Climate Change", in *Bitcoin Magazine*, available at [1668] Guest author, "The History and Evolution of Proof-of-Stake", 2017, Cointelegraph. See also www.wenmerge.com [1669] For the Ethereum blockchain and since the end of 2022 (*see* below), a *validator node* must send a significant amount of ethers (33 ethers or around $60,000) on the following *smart contract* in order to hope to be randomly selected to validate a block and then obtain the associated reward (in ethers).

with varying degrees of success, this Appendix focuses on updating the Ethereum blockchain, which has been gradually implementing this mechanism for several years.

Ethereum is a public blockchain with its own digital token called "*ether*" (which operates in much the same way as Bitcoin). Although closely linked to the Bitcoin story, the Ethereum blockchain now differs in its purpose and operation. Ethereum aims to become a decentralized global infrastructure for the development of untrusted applications, offering dedicated computing and execution power for so-called decentralized applications. To use this new distributed architecture, it is necessary to use its native token, the ether. In addition, users of this blockchain can create other non-native tokens for their own use[1670] , by paying a transaction fee in ether (native token), to issue or exchange these first ones. Since its launch on July 30, 2015, Ethereum has become a kind of IT laboratory dedicated to Finance 3.0, i.e. a new digital space devoted to the progressive *tokenization of* society. This 3.0 network and computing sandbox allows for comparatively more use cases than the Bitcoin blockchain, as Ethereum is complex, hybrid (semi-decentralized), but scalable, while Bitcoin offers, for the record, a resilient and reliable cryptocurrency, but less scalable for the time being. It is essential to note that the Bitcoin blockchain is more decentralized than the Ethereum blockchain, a similar observation also concerning their adjacent application ecosystems[1671] . This implies that Ethereum's relative centralization can be precisely targeted by regulators, governments or hackers, while the overall resilience of the Bitcoin protocol makes such a quest for centralization in theory far more complex, if not impractical.

Since its launch, the Ethereum Foundation[1672] has planned and undertaken a number of complex upgrade phases to support the Ethereum protocol, with these enhancements then being implemented by "*core developers*", most of whom are funded by the Foundation. Since 2022, there have been five such development phases: "*The Merge"* (December 2022), "*The Surge"* (2023), "*The Verge*" (2023), "*The Purge*" (2023) and "*The Splurge*" (2024)[1673] . Although the technical details of each of these updates are complex, together they represent the ambitious promise of a blockchain that was initially public, became hybrid and finally became public again with this new PoS mechanism. If successful, Ethereum could position itself and respond in a novel way to the incompatibility triangle studied in the first part of this research. Since its major update in December 2022 (The Merge), Ethereum no longer uses the Proof of Principle mechanism.

[1670] These tokens are in a sense sub-tokens (non-native), i.e. they are backed by ether (the native token), but in some cases have their own characteristics and synergies.
[1671] See Appendix 7, *below*.
[1672] Ethereum Foundation, *v*. Ethereum.org
[1673] Ethereum, "Ethereum upgrades (formerly 'Eth2')", *v*. Ethereum.org

Bitcoin, but has replaced it with the aforementioned Proof of Stake mechanism, whose operation can be summarized in five steps:

(i) Users store their tokens (ethers) on their own node (conventional computer), or more often on that of a third-party online service. This step is mandatory for the node to be considered operational by the network.
(ii) Eligible nodes compete to build the transactions for the next block, provided they have complied with the previous step.
(iii) The Proof of Stake protocol randomly selects a node to validate and "*forge"* each new block.
(iv) The reward in ethers and other data are temporarily sequestered until other honest nodes verify the validity of the transactions.
(v) This reward is released and sent to the (honest) validator node that forged the block, but only when the network knows that the transaction is not incorrect or fraudulent. At this stage, there are several possible remuneration mechanisms (calculation and variable distribution of this reward according to certain situations).

On the basis of this non-exhaustive information, it is emphasized that PoS leads to a tendency towards centralization, i.e. this sequestration method has the effect of concentrating network validation and control in the short and medium term with holders of large quantities of tokens. In other words, according to the algorithms governing PoS, the more tokens a user possesses and sequesters on his node, the more likely he is to be selected to validate blocks, which implies a centralization of this validation mechanism with the players who possess the most ethers (an observation which can in theory be exploited maliciously to corrupt the network, for example by targeting these most important holders). To illustrate, in August 2022, the US Treasury sanctioned the online service Tornado Cash[1674] (now accessible again), an open source software program enabling the highly pseudo-anonymous[1675] sending and mixing of ethers on the Ethereum blockchain. This action led the U.S. Treasury to place several ethereum addresses on the *Office of Foreign Assets Control*'s *(OFAC)* blacklist, barring their owners from all online services, including the transfer of their funds in ethers. This general ban on this anonymizing service affects not only malicious users (illicit activities), but also and above all the majority of bona fide users who simply wish to reinforce the protection of their online privacy. In addition, this decision raises crucial questions for Ethereum's validator nodes involved in validating - as a reminder, automatic and non-discriminatory - transactions attached to illegal activities.

[1674] U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash", 2023. Available at
[1675] V. *Supra*, I, Title 2, 1.4.1

illegal. For example, will a validator managed by a company registered in the United States be considered responsible if he includes in a block - without his knowledge - a transaction originating from an address identified as suspicious or prohibited? If a validator signs the block of another validator who has included transactions originating from prohibited addresses, will he also be considered responsible and consequently sanctioned?

In light of these initial legal findings, the risk of potential censorship of all or part of the Ethereum blockchain's blocks or transactions by the US government is therefore particularly worrying, given that two-thirds of the validator nodes - now in PoS - of the Ethereum blockchain are located in the USA. If the US government decides that validators are required to censor certain transactions, this would jeopardize the very principle of decentralization of this blockchain. Indeed, in the event of suspected money laundering by a user, 66% of Ethereum validators would be legally obliged to exclude these transactions from[1676] blocks, while the remaining 34% would lose their sequestered ethers if they attempted to include and validate that same block that contained one or more allegedly illicit transactions. Should this trend strengthen, or even spread to other international jurisdictions, this latent political and state threat also observed in Europe could represent an existential threat to all consensus mechanisms, including Proof-of-Work, which is already under threat of prohibition due to its energy consumption.

Although the resilience and security guarantees of Proof-of-Stake (PoS) therefore seem inferior to those of Proof-of-Work (PoW)[1677] , it is possible that the resulting centralization will be reduced in the long term, which would mean that the computing promise of the Ethereum blockchain has worked. However, this would require the PoS to deliver on its complex technical promises in terms of scalability, volume and response time, as described in this study. If this happens, the PoS mechanism could become more decentralized, with potential benefits that would bridge the long-term security and resilience of the Ethereum blockchain. However, while PoS is likely to prove its technical worth over the long term, it will probably not match the resilience, decentralization and stability of the Bitcoin protocol and its PoW mechanism[1678] . In this respect, every player involved in the blockchain ecosystem

[1676] The following website allows you to track in real time the percentage of blocks complying with the LCB-FT rules enacted by the OFAC and validated on Ethereum (by players forced to be compliant on pain of sanctions, such as the *Tornado Cash* project mentioned).
[1677] SZTORC Paul, "Long Live Proof-of-Work, Long Live Mining", 2014, in Truthcoin.info,
"For the foreseeable future, there is no significant alternative to proof-of-work (...)", available at [1678] A study dated August 16, 2022 shows that 65% of Ethereum nodes are hosted in centralized data centers ("*data centers*"). According to the study, two-thirds of these come from three major web services data providers. The study also revealed that centralized web providers control the vast majority of the 4,653 active Ethereum nodes. This can expose Ethereum to central points of failure. In addition to the 69% of modes hosted on the Ethereum backbone, Amazon Web Services (AWS) hosts over 50% of Ethereum network nodes. In addition, over 15% of nodes are hosted by Hetzner and 4.1% by OVH. Geographical centralization is also a major issue for the Ethereum blockchain: the USA and Germany geographically concentrate Ethereum nodes, accounting for 46% and 13% respectively, KASSAB Sami. "Do Ankr and Pocket Solve Web3's Node Centralization Problems?", 2022, available at messari.io. See also CRYPTOJON, "Ethereum: Le Mensonge De La Ultra Sound

is looking for a minimum degree of IT resilience that a blockchain must meet (often referred to and assimilated by the term immutability). The question is whether Ethereum can guarantee such a threshold today. For example, it seems that Financial Services 3.0 is primarily concerned with building online services on a robust, future-proof and truly decentralized IT foundation, despite the limited scope for applications and use cases. In conclusion, while Ethereum currently offers use cases that Bitcoin does not (smart contracts, decentralized finance, stablecoins), its ecosystem of distributed applications built on Ethereum remains immature and subject to relatively significant social, economic and legal recentralization. What's more, Ethereum's decentralized applications are likely to face competition from future upgrades of the Bitcoin protocol (Lightning Network, Taproot, Taro, Ordinals). However, this latent 'censurability' of the Ethereum protocol and its applications[1679] seems to be an opportunity for the use case of distributed digital identity, which requires a certain guarantee by the public authorities regarding the issuance of root identity attributes. Thus, as Ethereum's co-founder himself admits in 2020, the PoS promise of value is still in its infancy: "*The difference between Bitcoin and Ethereum is that Bitcoiners consider Bitcoin to be 80% finished, but Ethereans consider Ethereum to be 55% finished*"[1680] .

Focus 3: *Proof of Authority (PoA*)

Whether Proof of Work or Proof of Stake, these two mechanisms are today mainly adopted by public blockchains. Private and hybrid blockchains use other consensus mechanisms, the predominant one being *Proof of* Authority *(PoA*). By way of illustration, blockchain companies and consortia such as EBSI[1681] , BCN[1682] and Alastria[1683] use this consensus mechanism. As the name suggests, this is a consensus mechanism that grants a few organizations the power and authority to generate and then validate the blocks of a blockchain. In other words, PoA requires its stakeholder organizations to designate a number of them as duly identified authorities responsible for validating the network's blocks. The identity of participating nodes and players is thus revealed and limited according to the trust that the reputation of each of them can legitimately inspire in all the infrastructure's stakeholders. When this reputation is high, a node will have full block validation and verification capabilities, whereas in the opposite case, only a verification function is generally assigned. Although this mechanism enables

---

Money " [Video]. YouTube. See also MoneyRadar Crypto. "Ethereum Threatened The Biggest Risks Facing ETH," 2023, [Video]. YouTube

[1679] V. Appendix 7.

[1680] LOCKE Taylor, "Vitalik Buterin says Ethereum will be '55% complete' post-merge", 2022, in finance.yahoo.com

[1681] V. *Supra*, I, Title 1, 2.2.2.2

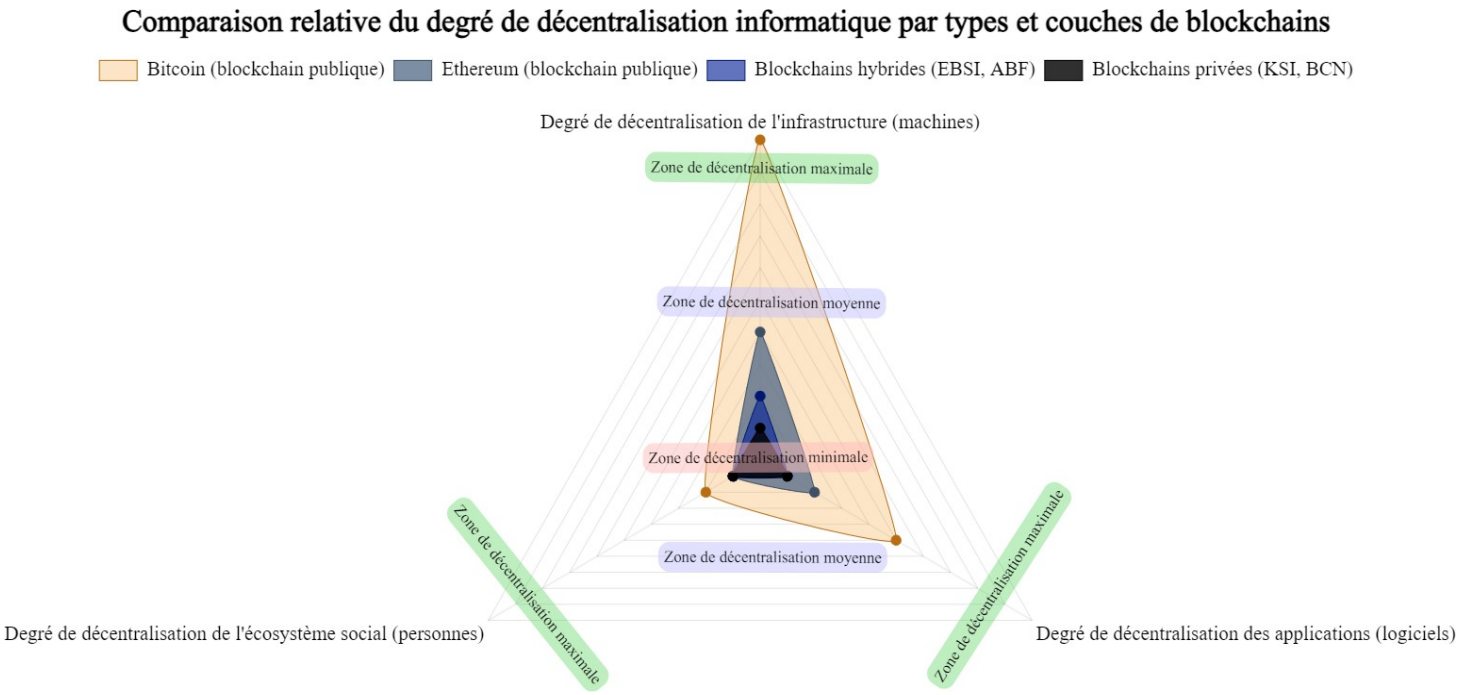
[1682] V. *Supra,* I, Title 2, 2.8

[1683] V. *Supra*, I, Title 1, 2.2.2.1.d

organizations to design a customized IT network that complies with current regulations (RGPD, eIDAS, MiCA, Data Act), it nevertheless only enables the creation of weakly decentralized blockchains. Indeed, we have found that for consortia networks of this type, the optimal number of nodes is only a few dozen. Beyond this number, these networks face difficulties that are difficult to resolve[1684] . This difficulty is also applicable to public blockchains, but these can respond more effectively thanks to their experience effect and the size of their developer communities. The consensus mechanism used can be compared to a voting protocol in which each user has a predefined voting weight, based on the reputation of each of the actors involved. In short, the PoA mechanism is suitable for organizations with a limited number of members who need to collaborate via a more or less decentralized IT protocol. PoA offers full legal compliance, and can be adapted to legislative and regulatory changes thanks to digital voting systems specific to a supposedly scalable governance. In practice, the maintenance of these networks can be tedious and complex for their members, leading to substantial delays and unexpected additional costs. As a result, some hybrid blockchains choose to implement a digital token, publicly accessible or not[1685] , to finance and ensure the development of the infrastructure and its associated applications. This may blur the boundary between these hybrid blockchains and public blockchains in economic, IT and social terms, but it also opens up new possibilities for IT interoperability.

[1684] *Op. cit. By* way of illustration, the *Hyperledger Indy* blockchain achieves optimal consensus when 25 nodes are operational (very few compared with public blockchains), and at least 8 nodes out of 25 must be functional in order to ensure the continuity of said deployed blockchain (in other words, beyond 25 nodes functional risks exist for consensus), "Introduction to Hyperledger Sovereign Identity Blockchain Solutions: Indy, Aries & Ursa", accessed online on 14/10/2021.
[1685] This refers to the Arianee hybrid blockchain, which is an association under the French law of 1901 that issues a token/token to its members, which is also publicly accessible. For more information, see the following link

Appendix 7: Illustration of components and levels of decentralization by blockchain (2022)



Appendix 8: Summary table of the Kleros decentralized justice protocol

As a reminder, Kleros is a set of online arbitration services, designed to be decentralized using Ethereum blockchain technology. Using techniques such as game theory, crowdsourcing, pseudo-anonymity and decentralization, Kleros is capable of resolving a variety of disputes, making it a decentralized judicial system for the Web 3.0 era. The following table provides a summary of some of the guidelines mentioned in the section dedicated to this 3.0 solution[1686] .

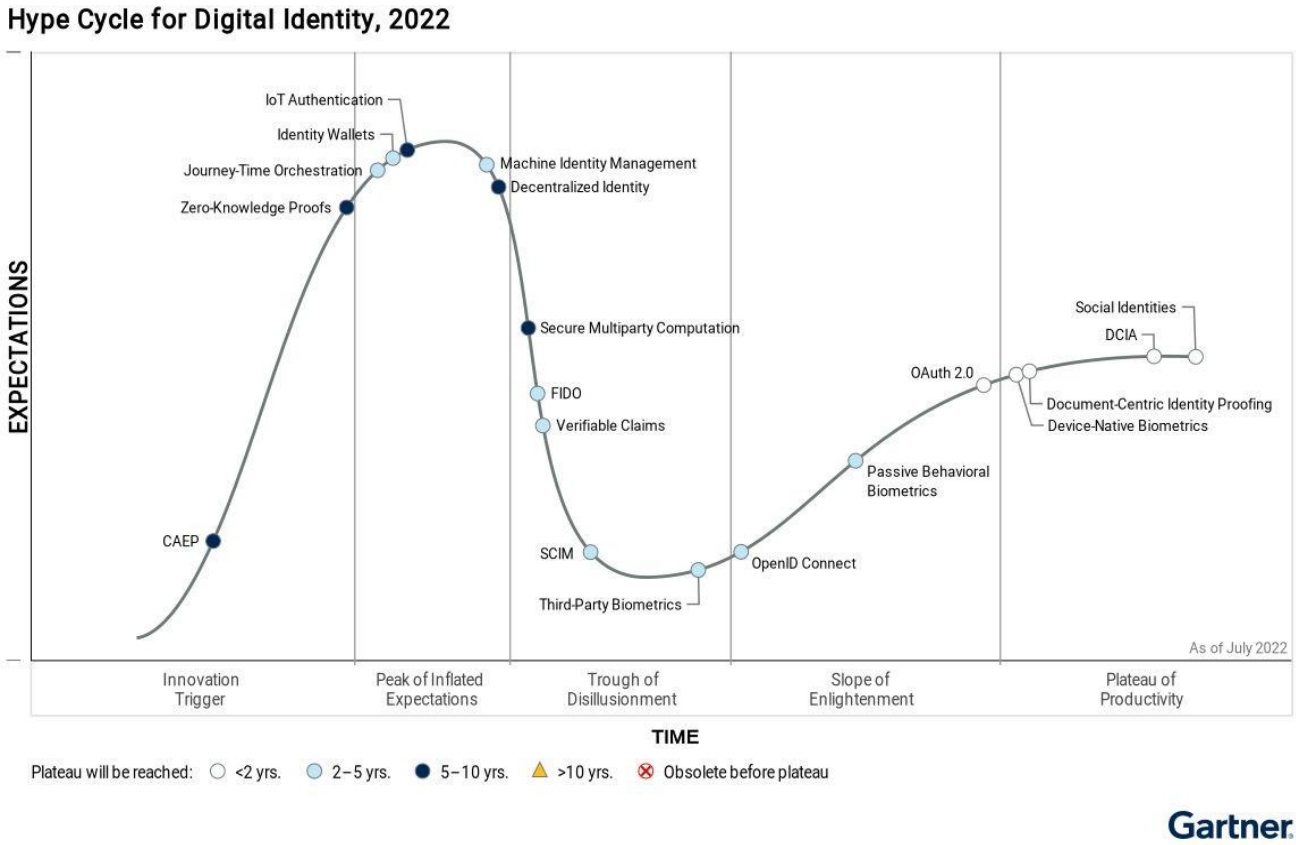
Questions	**Answers**
Is Kleros' *modus operandi* legally or morally right?	Kleros appears to be morally right in the eyes of its current community, which remains limited in number. However, the principle of community wisdom and economic incentive on which it is based depends on a minimum number of participants/users, which may vary over time and affect the collective decisions and truths rendered by the protocol. Although certain major principles of law serve as inspiration for the moral decisions taken by this protocol, the principle of territoriality of law is not respected (and does not appear to be intended to be in the short term).
Does Kleros comply with current legislation, i.e. is it legally recognized?	A priori, Kleros complies with neither the RGPD, nor eIDAS, nor the MiCA and TFR Regulations, nor the international arbitration rules set out in Article I Chapter 1 of the New York Convention[1687] , nor even the principles of territoriality. However, although the Kleros project is only at the beginning of its promise, gradual and partial recognition seems conceivable in the medium to long term, thanks in particular to a court ruling in Mexico and the European Innovation Council award won in 2020.

[1686] V. *Supra,* I, Title 2, 2.7.2

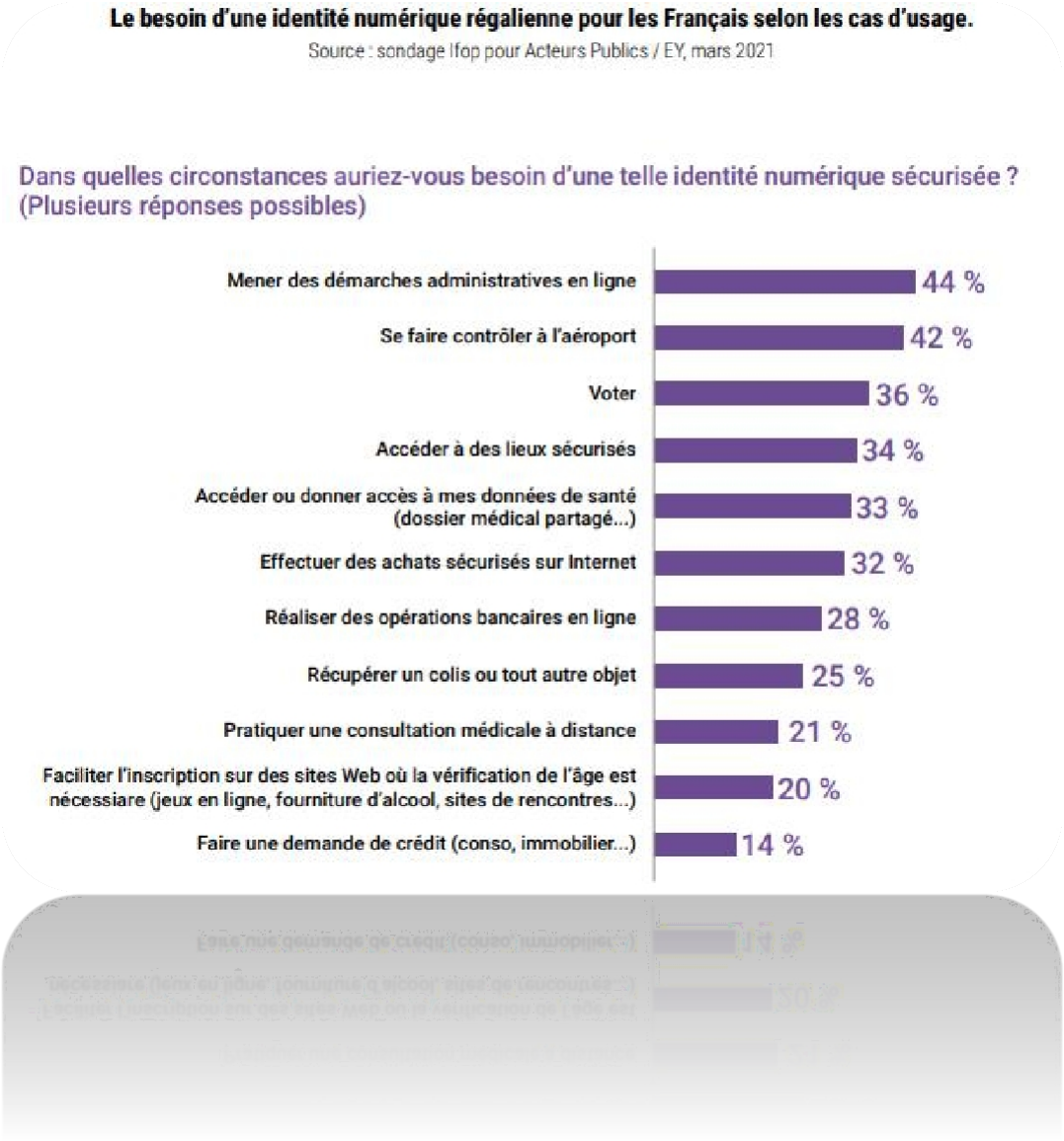
[1687] FERREIRA Leonel Constantino, "Blockchain dispute resolution: towards decentralized arbitration? ", published in January 2021, in *Master's thesis, University of Neuchâtel*, "Even if, depending on the circumstances of the case, a Kleros decision can theoretically be qualified as a foreign arbitral award within the meaning of the NY Convention, the procedure suffers from several anomalies preventing such qualification"; "When the Kleros procedure is delocalized, in the sense that it is not linked to a legal order, the New York Convention does not apply." p.96.

Is Kleros decentralized and open source? In terms of governance? Is the pseudo-anonymity of jurors guaranteed? Can Kleros be legally constrained or politically censored?	The Kleros protocol is more distributed than decentralized. Its protocol inherits a partial decentralization from the Ethereum blockchain (on which it depends), in the same way as Kleros smart contracts are relatively centralized due to the management of PNK tokens, which depend on the Kleros teams and their employees. In this respect, the anonymity of jurors is sometimes only a trompe-l'oeil, due to the groupings and influence that some of them exert among themselves on encrypted messaging systems (Telegram, Signal), which deviates from the supposedly wise, fair and impartial decisions. Yes, Kleros can be legally forced to cease part of its activities by court order. For example, their website and online communications are partly hosted on centralized platforms. The identity of the project owners is also (re)known, which means that political and institutional censorship would be possible.
Does Kleros amount to the financialization of online justice?	Yes, the compulsory purchase of PNK tokens to access the Kleros online service is tantamount to conditioning the decisions of this protocol to a forced financialization that many Internet users cannot afford, particularly in the developing countries targeted by Kleros. In other words, it's a far cry from the idea of decentralized online justice, accessible to all and free of charge.
To what extent is Kleros socially adopted, i.e. used by Internet users?	Kleros has been in marginal use since its launch. There are few users at present, as Kleros requires the handling and understanding of crypto-assets via more or less complex digital wallets. On the other hand, its use cases and positioning in the crypto sphere seem relevant, which raises hopes of eventual adoption (the latter also being conditional on the success of the Ethereum blockchain updates mentioned).
Can Kleros compete with and replace the current justice system?	Not unless our society becomes more digitized, as in the case of the advent of "*immersive metaverses*", an online political space that is lacking and could be implemented without at least partially abandoning the concept of anonymity, which is certainly necessary, but could also be rethought, as threatened by the Regulations mentioned.

Appendix 9: Digital identity trend cycle (2022)

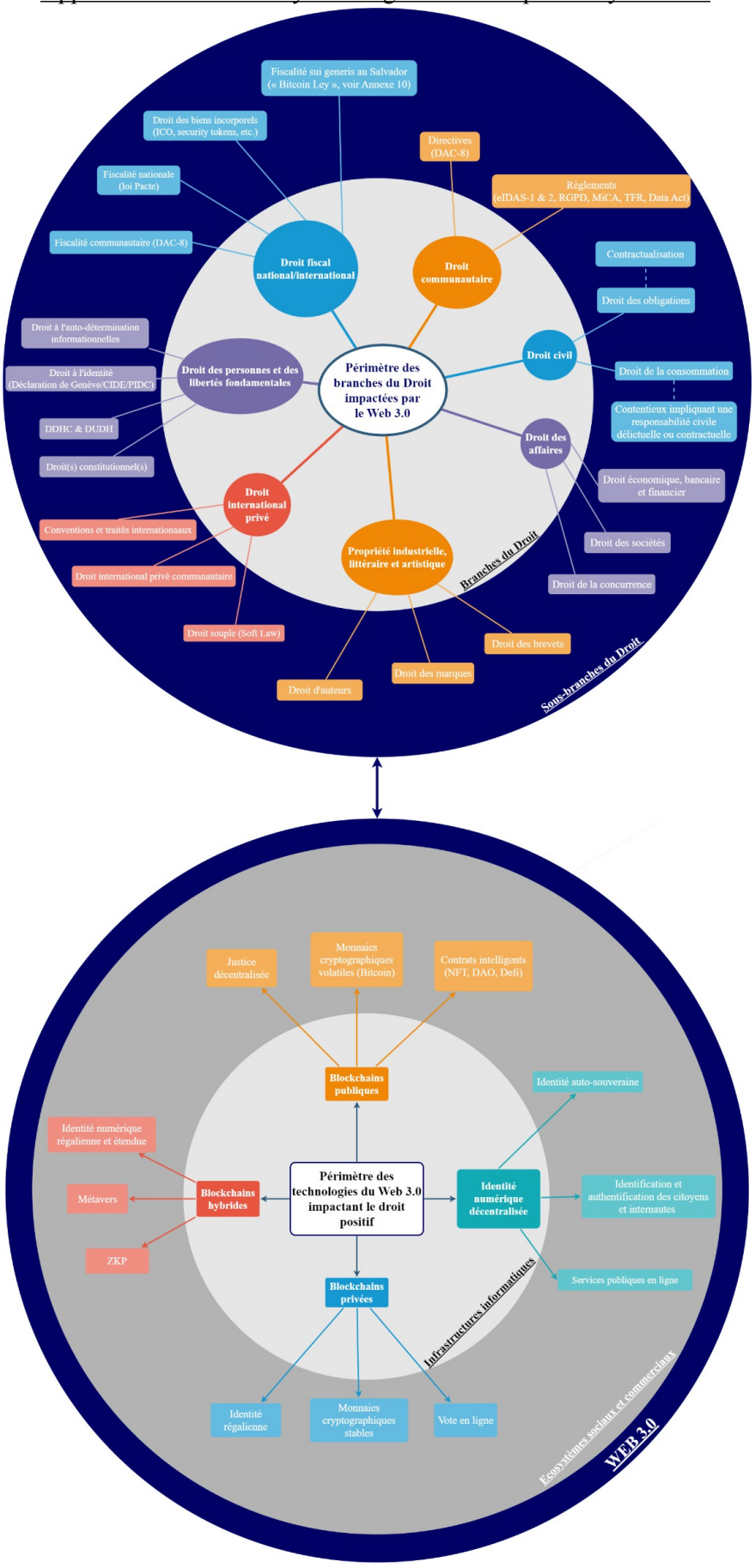


Appendix 10: French people's need for a regal digital identity, by use case

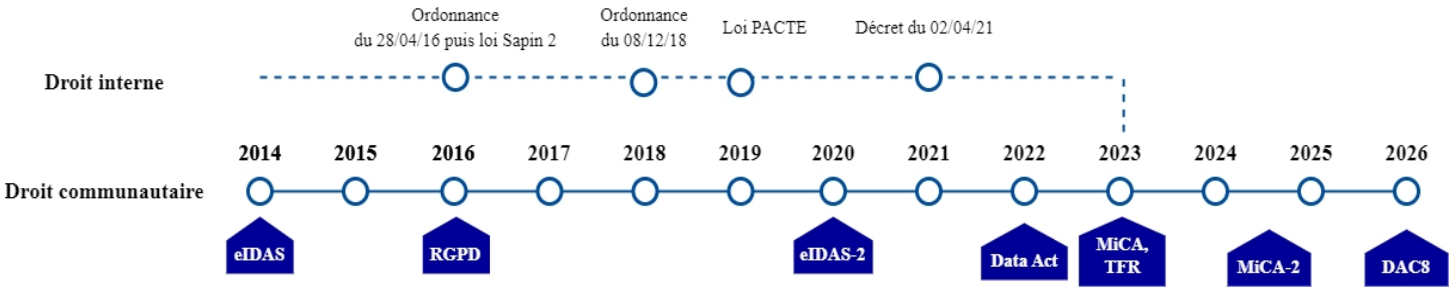


Appendix 11: Digital identity 1.0, 2.0 and 3.0 summed up in an image

Appendix 12: Cross-analysis of legal sectors impacted by Web 3.0



Appendix 13: Chronological timeline of national and European legislation on Web 3.0



Appendix 14: Regulatory status of crypto-assets by G20 country (2022)

G20+ Crypto Regulatory Tracker *August 2022*

Country	Crypto Framework	Tax	AML/CFT	Travel Rule	Stablecoin Reg	CBDCs
Argentina	🔴	✅	🟡	🔴	🔴	🟡
Australia	🟡	✅	✅	🔴	🟡	🟡
Brazil	🟡	✅	✅	🔴	🔴	🟡
Canada	🔴	✅	✅	✅	🔴	🟡
China	🚫	🚫	🚫	🚫	🚫	✅
European Union	🟡	🔴	✅	🟡	🟡	🟡
Hong Kong	🟡	✅	✅	🟡	🟡	🟡
India	🔴	✅	🔴	🔴	🔴	🟡
Indonesia	✅	✅	✅	🟡	🔴	🟡
Japan	✅	✅	✅	✅	✅	🟡
Mexico	✅	🔴	✅	✅	🔴	🟡
Russia	🟡	✅	🟡	🔴	🔴	🟡
Saudi Arabia	🔴	🔴	🔴	🔴	🔴	🟡
Singapore	✅	✅	✅	✅	🟡	🟡
South Africa	🟡	✅	🟡	🟡	🔴	🟡
South Korea	🟡	✅	✅	✅	🟡	🟡
Switzerland	✅	✅	✅	✅	✅	🟡
Turkey	🟡	🟡	✅	🔴	🔴	🟡
United Kingdom	🔴	🟡	✅	🟡	🟡	🟡
United States	🔴	✅	✅	✅	🔴	🟡

🔴 Regulatory process not initiated
🟡 Regulation underway
✅ Regulation in place
🚫 Prohibition

Source: ARMSTRONG Brian, President of Coinbase, August 22, 2022, in Twitter

This illustration shows the legislative trends relating to crypto-assets in the G20 member countries, with a particular focus on taxation (above "*Tax*"). Although most countries have taken steps in this area, the European Union appears to be ahead of the USA in terms of the adoption of the proposed MiCA Regulation and the proposed amendment to the TFR Regulation. However, the legal framework for stablecoins and MNBCs is still being developed by the EC, as studied. For the time being, China prefers to adopt a hostile legislative strategy towards crypto-assets. Switzerland, on the other hand, is gradually becoming a country of choice for entrepreneurs in this sector. Overall, the international framework of the crypto-asset market seems to indicate a tumultuous but gradual adoption by economic agents, who appear to be submitting to the rules of law in line with their business strategies.