TA SWISS

Programmed trust: Opportunities and risks of blockchain technology

Summary of the study «Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment»

TA-SWISS, the Foundation for Technology Assessment and a centre for excellence of the Swiss Academies of Arts and Sciences, deals with the opportunities and risks of new technologies.

This abridged version is based on a scientific study carried out on behalf of TA-SWISS by two project teams led by Nils Braun-Dubler as well as Antoine Burret. The abridged version presents the most important results and conclusions of the study in condensed form and is aimed at a broad audience.

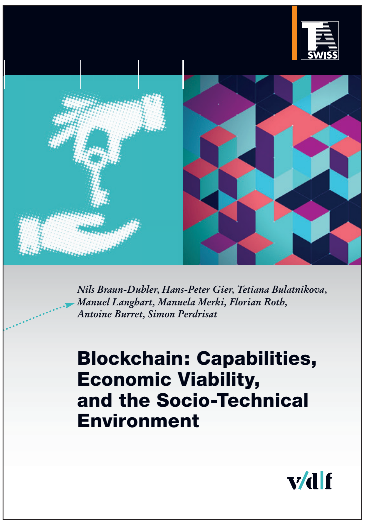
Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment

Nils Braun-Dubler, Hans-Peter Gier, Tetiana Bulatnikova, Manuel Langhart, Manuela Merki, Florian Roth, Antoine Burret, Simon Perdrisat

TA-SWISS, Stiftung für Technologiefolgen-Abschätzung (Ed.)
vdf Hochschulverlag an der ETH Zürich, 2020.
ISBN 978-3-7281-4016-6

Also available in open access: www.vdf.ch

This abridged version can be downloaded at no cost:
www.ta-swiss.ch



Nils Braun-Dubler, Hans-Peter Gier, Tetiana Bulatnikova, Manuel Langhart, Manuela Merki, Florian Roth, Antoine Burret, Simon Perdrisat

Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment

v/d/f

A brief introduction 4
Switzerland – a blockchain nation 4
A machine that manufactures trust 4
Opportunities of the blockchain 5
Risks of the blockchain 5
Dual focus 6

A look back 6

The links in the chain 8
A crash course in cryptography 8

A closer look at potential blockchain applications 12
National registers – digital guarantors of property rights 12
Cryptocurrencies – through the valley of disappointment 12
Initial Coin Offering (ICO) – a virtual stock market launch 13
Private payment systems – shopping in a refugee camp 14
Certificates of origin – from shore to plate 14
Smart energy management – the sun over Brooklyn 15
The hunt for a killer application 15

The blockchain as a catalyst 16
Trust, control, accountability 16
Transparency versus privacy 16
Taming the tiger – but as a collective 16

A brief introduction

Libra, the global payment system developed by Facebook, was supposed to be the big breakthrough: at last, the first blockchain-based application that could be used for everyday transactions. In the meantime, however, the signs for a mainstream use of blockchain technology are no longer very promising. Various major companies participating in the project – including Visa, Mastercard and PayPal – abandoned the project already before its planned start in 2020. Resistance to the novel currency is too strong, and central banks and governments have serious reservations about the parallel payment system – an inauditable "private global currency" – that functions without bank or governmental oversight and that could encourage money laundering, finance terrorism and destabilise the established financial system.

Switzerland – a blockchain nation

Switzerland has decided to focus on the potential held by blockchain technology, in particular the possibilities associated with innovative approaches in the financial market. Indeed, the country is well-positioned to benefit from blockchain technology: thanks to the liberal regulatory system in Switzerland, a dynamic community of blockchain pioneers has already established itself in "Crypto-Valley", located between Zug and Zurich. The country's flexible and liberal arbitration practices also have the potential to situate Switzerland as a major place of jurisdiction for so-called smart contracts. To strengthen and further develop Switzerland as a hub for blockchain technology, the federal government initiated a task force in 2017 and is committed to increasing legal certainty surrounding blockchain applications by means of targeted amendments to the relevant acts.

A machine that manufactures trust

Simply put, the blockchain is a forgery-proof decentralised database. Instead of traditional authorities and (often democratically legitimated) institutions that guarantee correct procedures in all transactions, the blockchain operates on the principle of trust among all participants in a transparent and (theoretically) absolutely fail-safe technological system. The greater the number of participants in a consensus process, the greater the trust – and the greater the protection against manipulation. This is why the blockchain is also called a machine that generates trust: a trust machine that aims to transform the internet into an "internet of values" in which items such as money, property titles, insurance policies or identity cards can circulate securely across the globe.

The virtual currency Bitcoin – followed by other cryptocurrencies – was the first application of the blockchain. Bitcoin is also quite certainly the application that has contributed most to the dubious reputation of the new technology. Many digital and financial experts were euphoric about the potential of what they believed would be the most important development since the creation of the World Wide Web; yet at the same time, tucked away in the dark corners of the internet, the illegal trading platform Silk Road was using Bitcoin to pay for its dubious dealings. There was also wild speculation, price fluctuations, unrealistic expectations on the one hand, and a stubborn lack of actual applications geared towards everyday use on the other – all factors that played a role in creating the hype and legends surrounding the blockchain. Another problematic aspect is the complexity of an IT system that most people simply do not understand. Lastly, the greatest advantage of blockchain technology is also its weakest point: because it dispenses with traditional supervisory authorities, the blockchain itself assumes the role of a trusted authority. But is it possible for a technical system to function as a "trusted third party" and thus be a viable replacement for governments or, depending on the area, for financial oversight, an election authority or a notary public? And can the blockchain truly serve to reform capitalism, as many of the technology's most avid proponents believe? The answers to these questions are socio-political in nature.

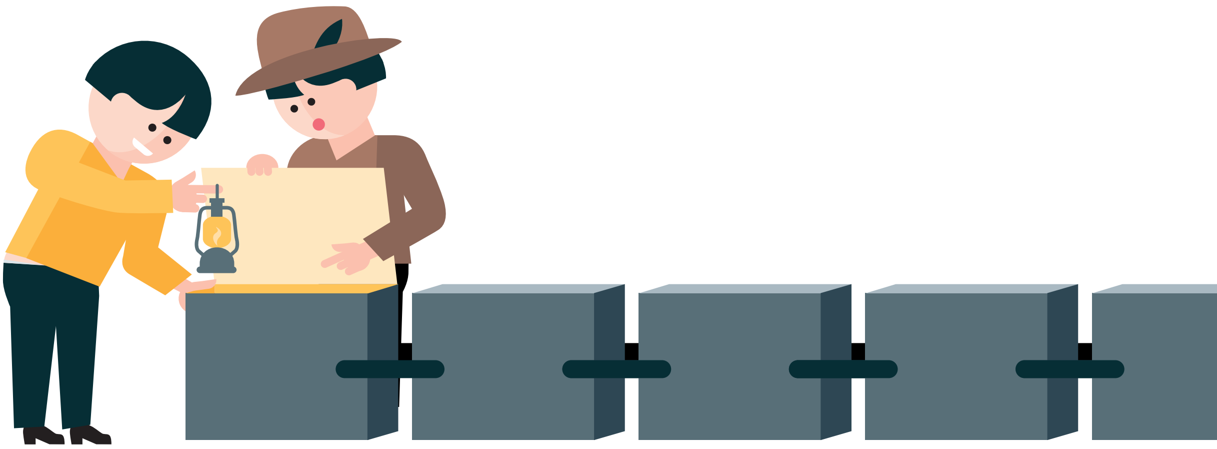
This is the set of conditions and questions that formed the starting point for the Foundation for Technology Assessment TA-SWISS – in accordance with its stated purpose on behalf of the political sphere and the general public – to compile comprehensive knowledge on the opportunities and risks of blockchain technology.

Opportunities of the blockchain

- Its immutability, which is secured via cryptography and a smart incentive system which ensures that all participants in a network guarantee the legality of all transactions.
- Its decentralised character, which makes the entire system manipulation-proof.
- Its ability to create trust among participants who are not (well) acquainted.
- Its ability to guarantee an absolutely verifiable and auditable digital record of property rights or certificates of origin. As such, blockchain technology has the potential to fundamentally restructure how financial services are provided.
- Its ability to provide faster, less expensive and more reliable transactions, as intermediaries would no longer be necessary.
- The transparency and immutability of the secured information, which increases legal certainty. This would be especially advantageous in countries where a trusted or efficient central authority is lacking.
- The fact that the blockchain – in conjunction with smart contracts and with the Internet of Things – enables automation of review processes and validation certificates.

Risks of the blockchain

- The fact that some of its consensus mechanisms used to replace a single trusted authority are distributed across a large number of computers, which requires an enormous amount of processing power and thus consumes a massive amount of energy.
- The anonymity of participants in public blockchains, or the use of a pseudonym. This could be misused for criminal purposes.
- The fact that all transactions of an individual can be tracked as soon as the identity behind a pseudonym is revealed.
- That its immutability precludes the right to be forgotten, which is stipulated in data privacy rules.
- The fact that its complexity makes it entirely impenetrable to non-specialists, although the blockchain promises greater transparency and collective decision-making.
- The fact that it remains largely a “solution without a problem”: to date, no “killer application” has been developed and the blockchain has failed to live up to expectations created by the hype surrounding the technology.



Dual focus

TA-SWISS is presenting a two-part study on blockchain technology. The first, more technical part provides an in-depth look into how the blockchain functions and examines the technology's economic potential. In addition, twelve case studies comparing blockchain applications to traditional solutions in the same sector show where the new technology brings actual benefits and where it (currently) fails to fully convince. The applications discussed include public land registers and payment systems in refugee camps on to energy supply systems. This first part of the study was conducted by a project team at the Institut für Wirtschaftsstudien Basel (IWSB) led by Nils Braun-Dubler in collaboration with the management consulting company Banking Concepts and MME, a company that provides legal tax and compliance advice. The second part of the study places the blockchain, its genesis and how it is perceived in a sociological and cultural context. This part of the report focuses on how social discourse on the blockchain is affected by the system's obscurity to non-specialists and examines who profits from maintaining a certain level of hype regarding the technology. The second study was written by Antoine Burret and Simon Perdrisat, sociologists at the Centre Universitaire Informatique of the University of Geneva.

Taken as a whole, the two studies constitute a comprehensive overview of the current situation that should help to calm the excitement and temper expectations, which are often just as exaggerated as the fears and defensive reactions around blockchain technology. In addition, these reports create a factual basis for the debate on the technology's economic and societal significance and for considering its current and future applications.

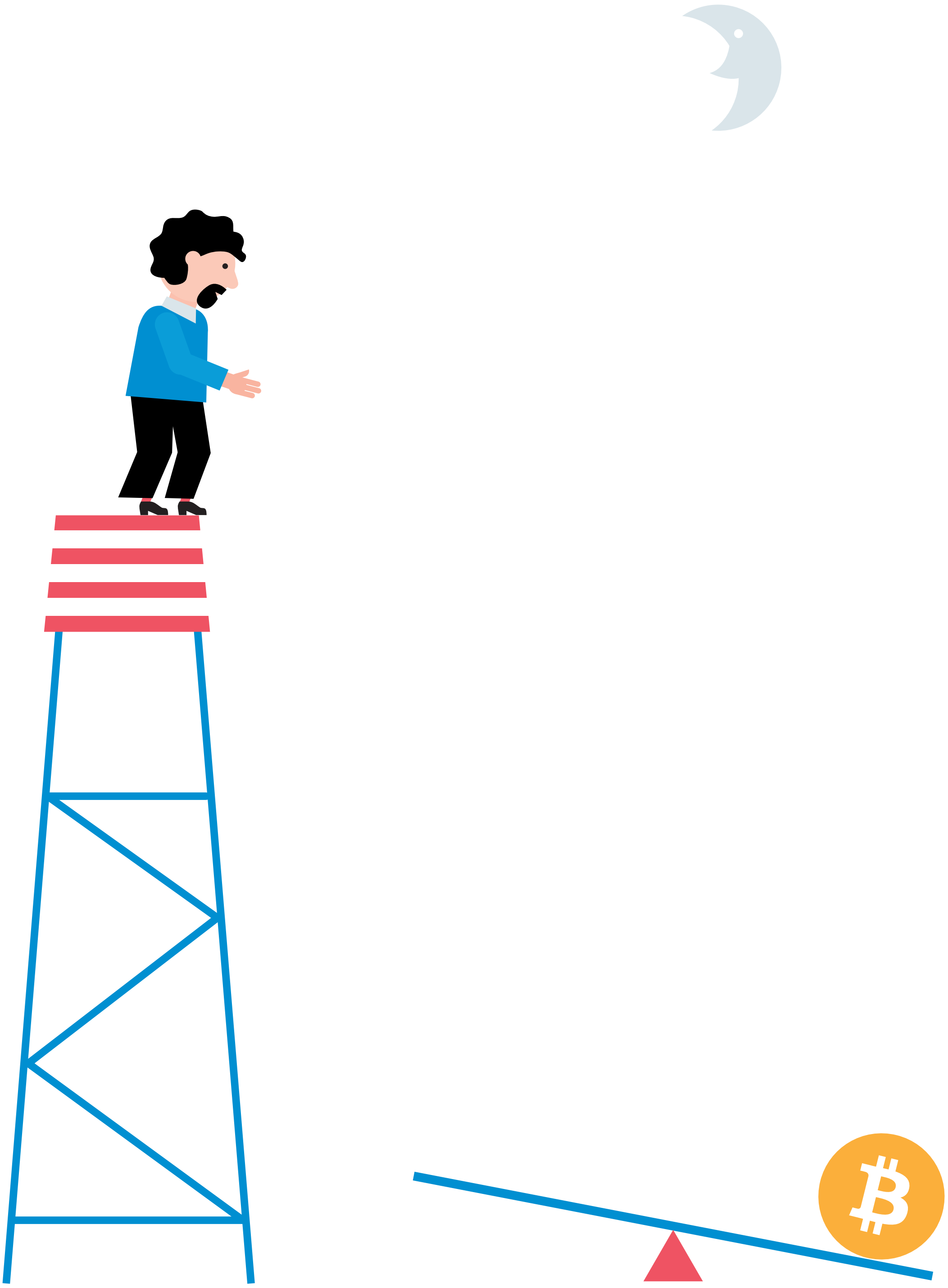
A look back

In 2008, the mysterious Satoshi Nakamoto – it remains unclear whether a single individual or a group of people is behind the pseudonym – published a scholarly paper on a mailing list dedicated to cryptographic technology. In the paper, the author discussed a new electronic monetary system able to transfer monetary values within a decentralised network using a chain of cryptographically secured data sets. The system is forgery-proof and it solved a fundamental problem that had dogged all previous digital currencies: preventing the same digital sum of money to be accounted more than once in a system that has no central supervisory authority. Nakamoto named his payment system "Bitcoin". With Bitcoin, the traditional, trusted intermediary is replaced by a cryptographic proof that uses a smart incentive system to encourage all users in a network to work on the proof and validate it. The paper – a modest nine pages – was received with enthusiasm.

Far from arising out of nowhere, Nakamoto's invention was built on concepts and theoretical considerations from mathematical cryptography and IT, combined with new technologies. At the same time, however, the novel currency also represented one of the most profound change brought about by the commercialisation of the IT sector: encryption methods that allow information to be exchanged securely, reliably and confidentially on the World Wide Web are no longer restricted to governments and large corporations; now they are tools that the entire digital society has laid claim to.

On 3 January 2009, Nakamoto mined the Genesis block of the Bitcoin blockchain. Shortly thereafter, "he" disappeared and handed over further development of the open-source Bitcoin software to the blockchain community. On the very first block on the chain, the enigmatic creator inserted a headline from the London Times alluding to the global banking crisis, making it clear from the outset that the Bitcoin project is not solely a technical development but also part of a social project that is highly critical of centralised government institutions.

Bitcoin inspired the development of numerous alternative cryptocurrencies, also called "altcoins", with names like Litecoin or Peercoin. But already in 2009, there were plans to expand the fundamental innovation behind Bitcoin – the blockchain – to applications beyond alternative currencies and financial transactions, for example, cargo ledgers, property deeds, diplomas. Anything which is (1) “representable as a digital asset”, and (2) a “rivalrous good”, meaning that only one person can own it at a time, is potentially fair game for representation in the Bitcoin blockchain, as software developer Vitalik Buterin stated in a White Paper from 2013. A few years later, these considerations led to the creation of a new platform: Ethereum, which is more than a cryptocurrency, more powerful than Bitcoin and capable of automatically initiating agreed transactions once certain conditions are fulfilled – for instance, it can transfer a payment as soon as goods are delivered. Smart contracts now enter into the equation.

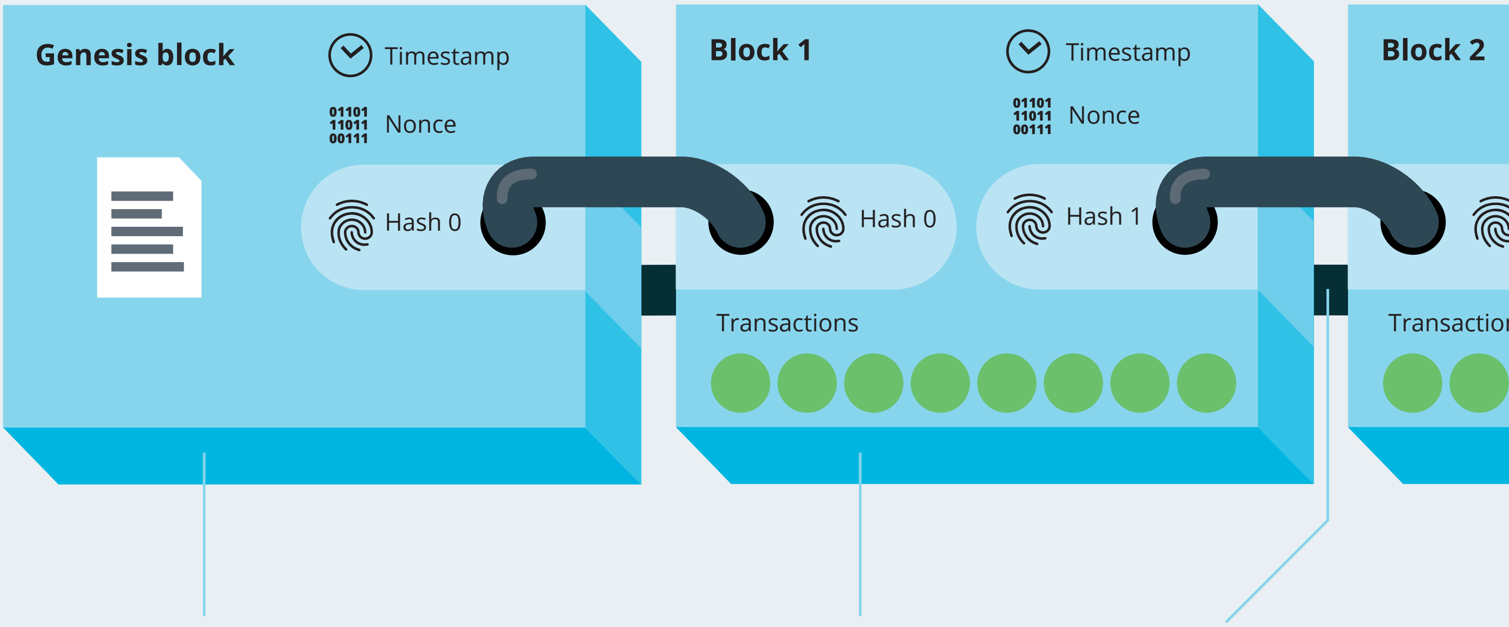


The links in the chain

Blockchain: an incorruptible digital ledger that is stored across a peer-to-peer network. It consists of a series of chronological hash values, each of which is linked to and references the previous hash value – a procedure that makes it impossible to retroactively alter blocks or unlawfully smuggle a block into the chain.

A crash course in cryptography

Cryptography: aims to secure and transfer data sets and sensitive information in a specific format so that unauthorised persons are prevented from gaining access to the data or are unable to understand the content (confidentiality). At the same time, the identity of both sender and receiver must be unambiguously verified (authentication). While being transmitted or saved, the data must remain verifiably consistent (data integrity) and, lastly, it must be ruled out that the authenticity of transmitted information can be disputed after a transaction is completed (non-repudiation). A secret key is used to encrypt and decrypt data. In symmetric encryption systems, both sender and receiver use the same key. In asymmetric encryption systems, two keys are used: a public key in addition to a private key that is owned by only one of the two transaction partners. In both cases, one key is used to retrieve the original data.



Genesis block: the first block on a blockchain. The consensus protocol is also defined in the Genesis block. The protocol specifies the tasks required for validating blocks, names who is authorised to do this work, and determines how frequently a new block may be incorporated into the chain as well as how large the block can be, i.e. how many transactions are stored on the block.

Block: the content of each block consists of the hash value common to all signed and stored transactions in a block, a timestamp and an arbitrary number (a “nonce”), which is used to validate the block. The hash value of the previous block is then added, and the hash value of the new block is calculated on the basis of all these values.

Chain: the individual blocks are linked using cryptography. Because each block contains the hash value of the previous block, the blocks form a chain in which all transactions are recorded, starting with the first block in the chain.

Hash function: a cryptographic method that, in contrast to encryption, is irreversible. A hash function is an algorithm that converts a file of any length and complexity (for instance, an entry in a public land register, a photograph or even an audio file) into a fixed-length sequence of characters (a "string"). SHA-256, the most common algorithm in the blockchain community, has 256 bits or characters; put differently, it is a sequence of 256 ones and zeros. Hashing mechanisms play a key role in blockchain technology.

Hash value of data input:
Hello World

```
10100101100100011010011011
01010000001011111101000010
00000100000001001010000000
01000101110011001111001111
10110111101100011001000011
01011000101100011001011011
11110000101111001101101000
11001010110101011110110010
01110111110110011010110110
0111110001010001101110
```

Hash value of data input:
Hello, World

```
00000011011001110101101011
00010100111111111110011100
11010001010100110101110011
00110001111101111111001101
11111010001011000100010110
00110001010010000110000011
01110001111101000001100011
01110000010011011011110010
11010001100110101100000111
1110111110100010100101
```

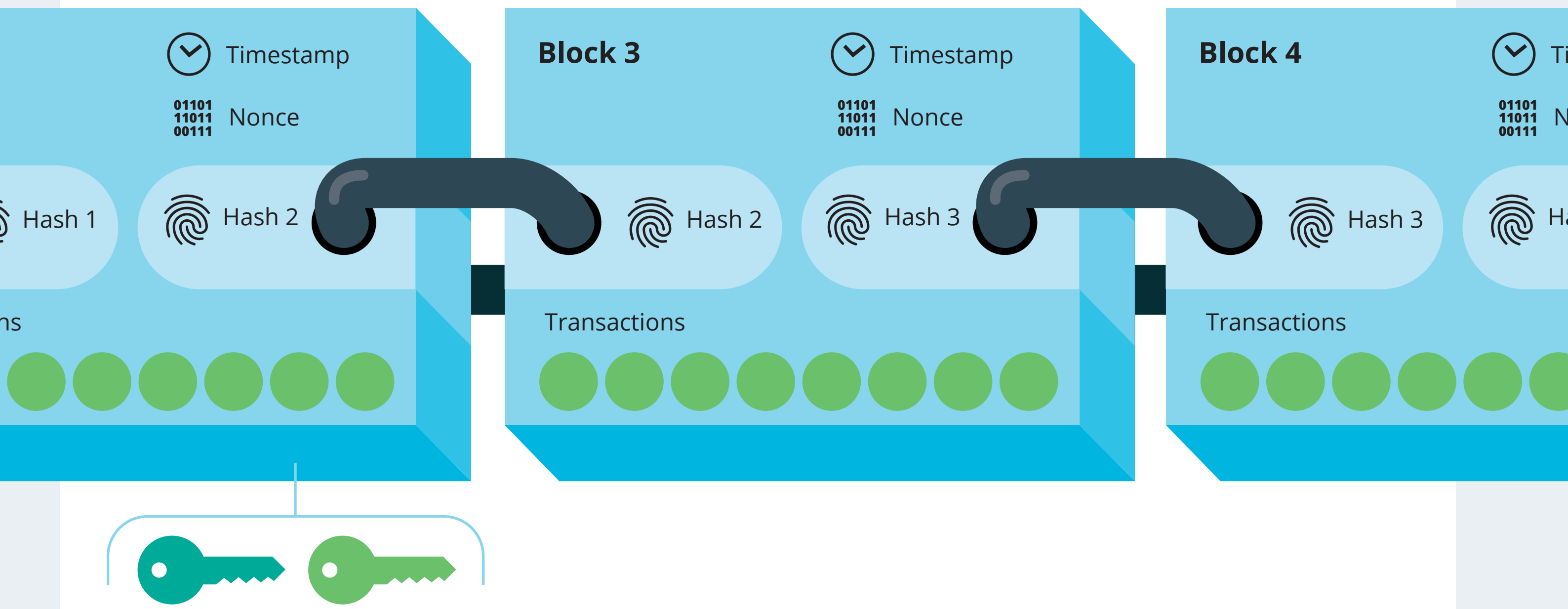
One hash, also called a check sum, has three major properties:

1. It is irreversible, meaning it is impossible to calculate back from the output to discover what input file generated it. As such, a "hashed" document cannot be reconstructed from its hash value. This, however, could change once powerful quantum computers are available: the tedious process of integer factorisation – which is impossible even for today's most advanced super computers – would be child's play for a quantum computer.

2. The smallest modification in an input yields an entirely different hash value, making it possible to determine whether a data set has been altered. Hash values can therefore expose manipulation.

3. The same input always generates the same output, which is why the hash value is referred to as a "digital fingerprint". If an output is different, it without exception means that the input values were changed.

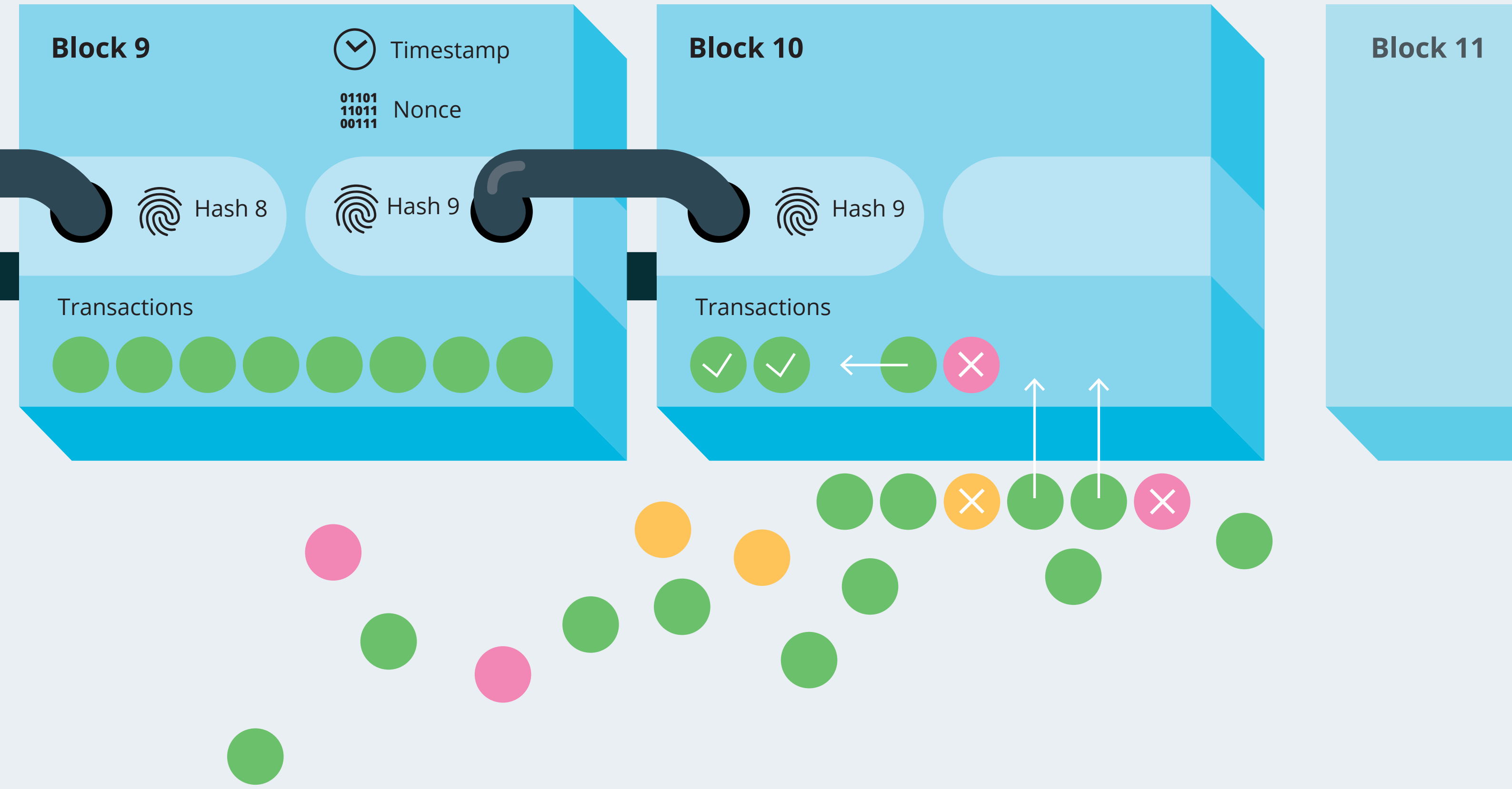
The power of big numbers: purely theoretically, the information in point 3 is not always true. It is possible that different data sets can be represented by the same hash value. The probability of such a collision is, however, so low that it can be disregarded immediately: it corresponds to the chance of winning the EuroMillions lottery nine times in a row. Equally, the probability that, for instance, two blockchain users would be assigned the same hash value for their account numbers is virtually zero.



Asymmetric encryption: used in blockchain technology to secure login data and verify ownership rights. Each user is assigned an arbitrary numerical combination as a "private key". This serves as the basis for calculating a "public key" and, from the latter, an account number (a "public address"). A user can use the private key as proof of being the sole authorised holder of a specific account. In addition, the user must use the private key to sign every transaction processed on his or her account. The mathematical link between the two keys makes it possible to check the public key to see whether a transaction was carried out correctly and a valid signature was used. If the account holder loses the private key, he or she can no longer access the account. An estimated three to five million bitcoins have been lost forever due to forgotten private keys.

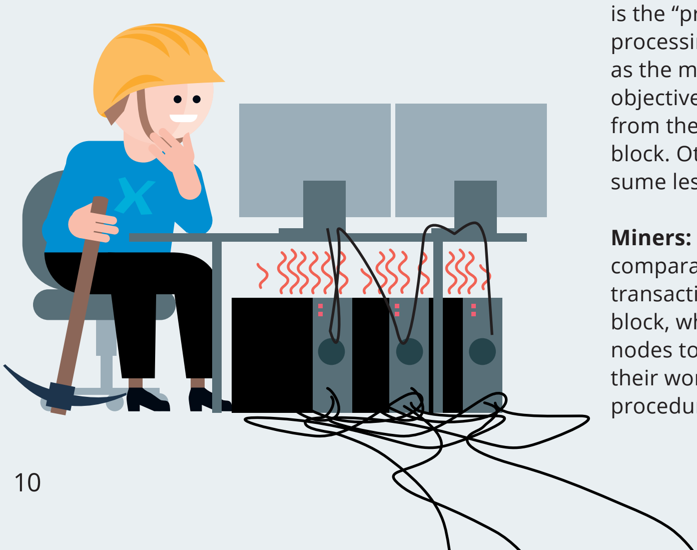
Pseudo-anonymity (pseudonymity): because the blockchain is transparent, all transactions can be tracked at all times, and they can be linked to a public address. To protect the privacy of users, the public key of a user is not associated with that individual's name but rather with a pseudonym that cannot be traced back to an actual person. Because it is nevertheless impossible to exclude that a user's identity can be deduced from his or her transaction history, the term "pseudo-anonymity" is used.

Zero-knowledge-proof: a mathematically daunting and complex cryptographic procedure in which one of the transaction partners proves to the other that he or she knows a secret without, however, having to reveal the secret. Zero-knowledge protocols can strengthen anonymity on the blockchain.



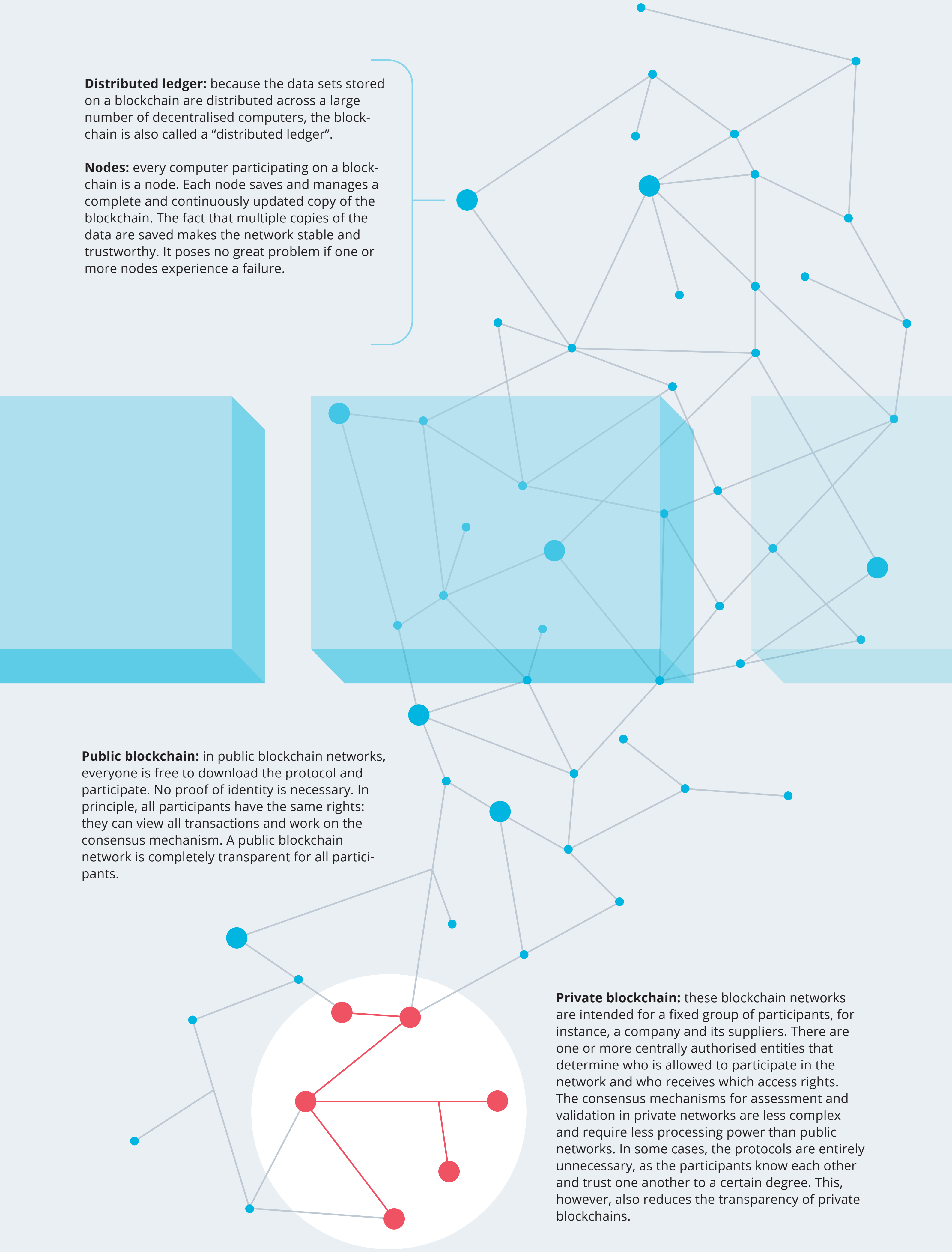
Consensus mechanism: in blockchain technology, a consensus mechanism replaces a central supervisory body. With this procedure, all participants decide which transactions are valid and in which order they will be introduced onto the chain. Not all blockchain applications use the same consensus mechanism. The most common procedure is the "proof-of-work" protocol, which requires a massive amount of processing power because each node is in competition with the other as the miners attempt to solve a complex mathematical problem. The objective is to calculate a unique hash for the next link in the chain from the pending transactions and the hash value of the previous block. Other consensus mechanisms are less elaborate and thus consume less energy.

Miners: some of the nodes are active as validators. Their task is comparable to that of an accountant: they assess the validity of new transactions, group them and cryptographically secure them as a new block, which they then incorporate onto the chain. To encourage the nodes to participate in the verification process, miners are paid for their work. In the case of Bitcoin, they are paid in new bitcoins. The procedure is often compared with prospecting for gold.



Distributed ledger: because the data sets stored on a blockchain are distributed across a large number of decentralised computers, the blockchain is also called a "distributed ledger".

Nodes: every computer participating on a blockchain is a node. Each node saves and manages a complete and continuously updated copy of the blockchain. The fact that multiple copies of the data are saved makes the network stable and trustworthy. It poses no great problem if one or more nodes experience a failure.



Public blockchain: in public blockchain networks, everyone is free to download the protocol and participate. No proof of identity is necessary. In principle, all participants have the same rights: they can view all transactions and work on the consensus mechanism. A public blockchain network is completely transparent for all participants.

Private blockchain: these blockchain networks are intended for a fixed group of participants, for instance, a company and its suppliers. There are one or more centrally authorised entities that determine who is allowed to participate in the network and who receives which access rights. The consensus mechanisms for assessment and validation in private networks are less complex and require less processing power than public networks. In some cases, the protocols are entirely unnecessary, as the participants know each other and trust one another to a certain degree. This, however, also reduces the transparency of private blockchains.

A closer look at potential blockchain applications

National registers – digital guarantors of property rights

At first sight, the blockchain's properties as an incorruptible and completely transparent digital ledger appear to make it a particularly apt solution for national registers such as the public land register. Distributed across numerous computers, blockchain-based registers guarantee the immutability of all information logged and offer greater security than a database stored on a central server. In addition, transactions are processed more quickly and efficiently, and a central authority is rendered unnecessary. These aspects can represent a great advantage in countries with weak legal institutions.

But what about Switzerland? An example of a national register in Switzerland would be the public land register, which maintains a record of the rights associated with a parcel of land. Every change, be it the sale or transfer of land to a new owner, must be notarised and entered into the register. There is no Swiss-wide land register; instead, the cantons are responsible for maintaining a public land register on behalf of the federal government and for guaranteeing that all entries are correct. The public land register is a public record – anyone can ask for information about who owns a specific parcel of land, meaning that the public land market is largely transparent. As such, the public land register appears to already share many of the blockchain's strengths.

An additional aspect is that the right to privacy protection laws limit who may view the public land register: it remains in the discretion of the cantonal land registry offices to give wide-ranging access to individuals who can credibly claim a valid interest. Without changing the law, this feature could only be reproduced by using a private blockchain with precisely defined access rights. In this scenario, trust in cantonal land registries would be replaced by trust in a group of authorisation entities.

Completely transferring a national register to the blockchain makes little sense. More interesting are partial solutions such as the approach being tested in the Canton of Geneva. There, land register excerpts that have been requested by citizens are simultaneously logged on the blockchain, allowing persons making the query to verify whether the document they were sent matches the original and is thus valid. Nevertheless, the SuisseID – Switzerland's already existing and legal electronic identity card – could serve the same purpose. A more promising approach is expanding the functionality of a blockchain-based register by using smart contracts: in such cases, changes in a public land register would be legally valid only after specific conditions have been met.

Cryptocurrencies – through the valley of disappointment

In 2017, the value of Bitcoin – the most important digital currency – exploded, increasing by over 1,800 per cent to a record high of 20,000 US dollars by the end of the year. Other cryptocurrencies – there are some 3,000 different kinds to date – are also susceptible to rapid price increases followed by steep drops in value. And attitudes in the public sector, financial markets and governments towards the novel asset class demonstrate a similar volatility: on the one hand, a great future is predicted for cryptocurrencies, and there is much talk of their potential to revolutionise the entire monetary system and put an end to the hegemony of traditional banking institutions. Technology-friendly countries such as Japan have accepted cryptocurrencies as part of the up-and-coming fintech sector and, in Switzerland, the federal Financial Market Supervisory Authority (FINMA) has issued a banking licence to two crypto-banks. On the other hand, there are warnings of a classic speculation bubble, and some see a threat to financial stability as well as an audacious attempt to circumvent monetary authorities and regulatory bodies.

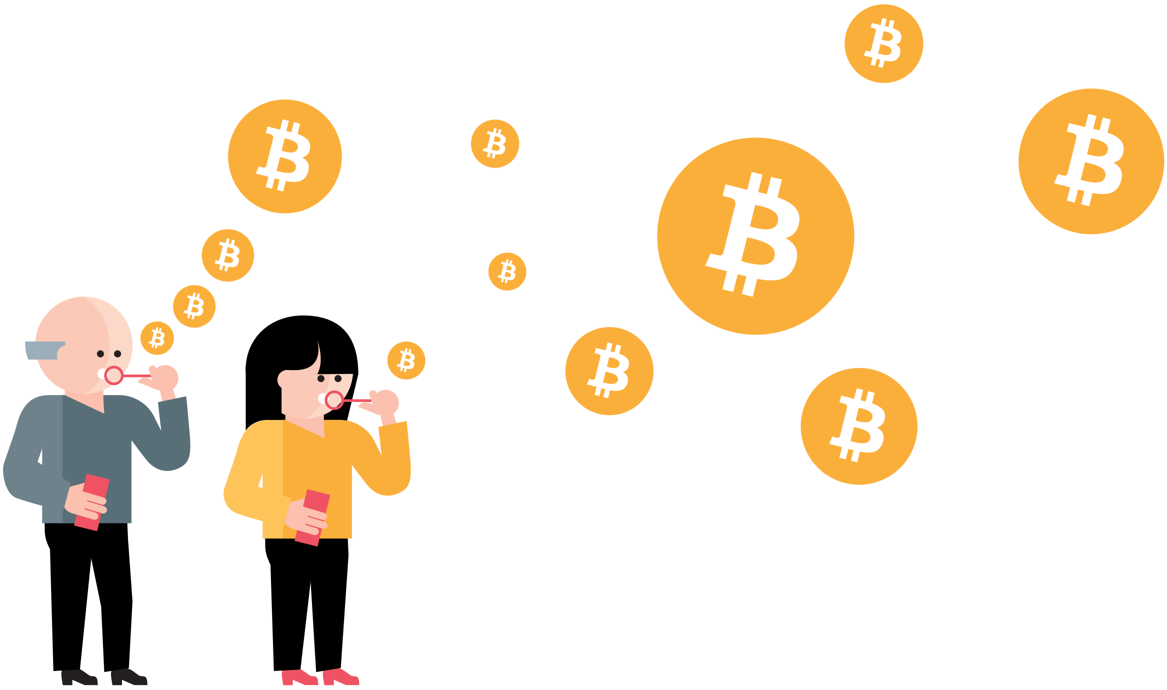
A sober look at virtual currencies, however, reveals that these payment systems in particular tend to underperform. To date, they offer a poor alternative to traditional currencies: their average daily transactional value is significantly lower, their stability is woefully inadequate, and they are still rarely accepted as a common payment method. They have also failed to replace traditional payment systems: globally, only about seven transactions per second can be conducted using Bitcoin, whereas PayPal payments are transferred almost instantaneously. As a “safe haven” asset, cryptocurrencies – which have no intrinsic value, in contrast to gold – are much too volatile.

The blockchain community is working on modifying and further developing cryptocurrency systems. For instance, the Bitcoin Foundation endeavours to standardise, promote and protect the worldwide use of cryptographic currencies. At present, however, the bottom line is that blockchain-based currencies have not yet lived up to their own expectations.

Initial Coin Offering (ICO) – a virtual stock market launch

Raising capital for start-up companies can be a difficult and protracted undertaking. Now, a funding opportunity has arisen in the blockchain community that combines blockchain technology with crowdfunding. In contrast to a traditional stock market launch – an Initial Public Offering or IPO – shares of a company are not traded against venture capital but for tokens, which are digital units of a cryptocurrency that was created specifically for the business being launched. FINMA differentiates between three categories of blockchain-based tokens: those with a monetary value (payment tokens), those that provide access to a service (utility tokens) and, lastly, those that represent the value of an asset (asset tokens). The buyer speculates that the future success of the supported start-up company will cause the value of the purchased tokens to multiply. ICOs meet with great enthusiasm on a global level, and they regularly set trading volume records. An ICO makes it possible to finance an original idea already at the very start of a project. This can represent an incredible opportunity to rapidly implement innovation – but it can also be a ruse to take money out of the pockets of naive investors.

A traditional stock market launch generally takes at least five months to prepare, is very costly and requires overcoming numerous administrative hurdles. In addition, an IPO is subject to stringent regulations and requires the intermediary services of at least one bank. By contrast, an ICO is comparatively simple, fast and inexpensive. Especially in Switzerland, where venture capital is not overly abundant, ICOs have given a boost to young companies in the fintech sector. That Switzerland has in the meantime become one of the major hubs for ICOs is primarily related to the favourable legal and taxation regulations, the thriving fintech scene and an outstanding talent pool in research at the country’s higher education institutions. To lower the risk of fraud – inherent due to the speculative nature of an ICO – FINMA has published guidelines that aim to clarify the situation and protect the integrity of the financial sector without, however, reducing the innovative potential held by the virtual stock market launches.



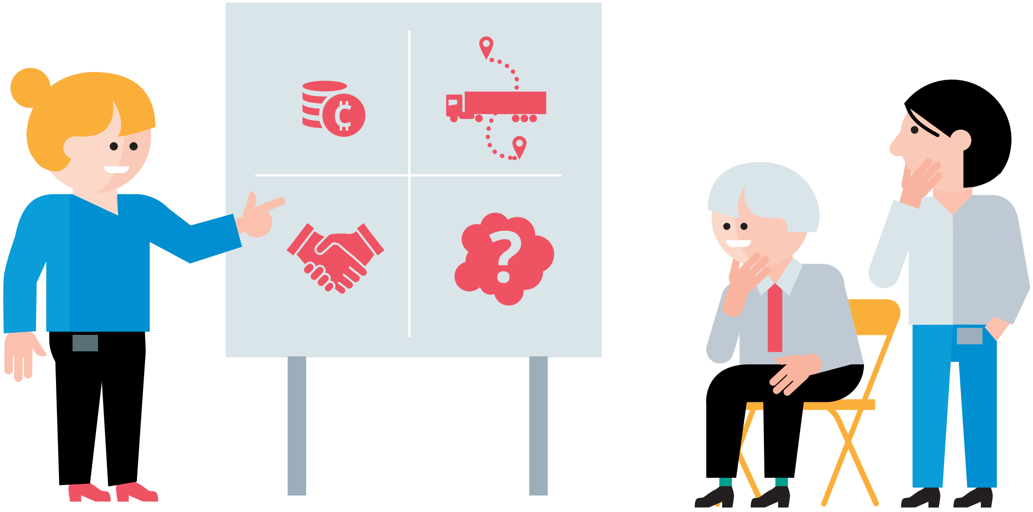
Private payment systems – shopping in a refugee camp

A very interesting blockchain project is currently being tested in the Azraq refugee camp in the Jordanian desert. The United Nations World Food Programme (WFP) introduced blockchain technology to distribute food to the roughly 10,000 Syrian refugees in the camp. About ten years ago, the programme stopped delivering rations directly and instead began giving refugees money or pre-paid cards to make their purchases. The new method helps to restore some autonomy and dignity in the lives of the refugees and has remarkably also led them to eating a more balanced diet. In addition, these "cash-based transfers" stimulate the local economy and save transport and logistics costs. Nevertheless, food vouchers can be lost, stolen or hoarded, and they can be resold at a profit. Since May of 2017, payments in the Azraq camp supermarket can be made with a blockchain-based system that is more secure and efficient – and also largely impossible to manipulate. Persons wishing to make a purchase use an iris scan to identify themselves. The data are compared in the WFP database, where information on the account, identity and shopping history of all refugees are logged as encrypted data sets on the blockchain. The intermediary position of a bank is no longer necessary: WFP takes on the role of the centralised authority that assumes sole responsibility for payment transactions and bookkeeping. This makes the entire procedure more efficient and less expensive, as no additional fees are levied.

The system used in Azraq is a rudimentary private blockchain network with a single node. At the camp, Blockchain technology is primarily used for forgery-proof storage of sensitive data. Nevertheless, it is possible that the highly successful project could be expanded across a decentralised network to access the full potential of the blockchain. It could be used to transparently process purchases and expenditures for various camps – and possibly even the services of other charities – in a single, decentralised system. Misappropriation of donations, siphoning money into the pockets of corrupt intermediaries or misappropriation of funds would be impossible.

Certificates of origin – from shore to plate

The blockchain can also help to better control the delivery routes of consumer goods and foods across complex supply chains. For instance, the British startup Provenance uses the Ethereum blockchain platform to validate the origin of responsibly fished tuna from Indonesia. To begin, a local fisher sends a simple text message to the system and registers the weight and quality of a catch. The criteria for sustainable fishing have been previously set by an independent certification authority that has also logged the information on the blockchain. All this information is used to create a token to identify the catch. This "digital fingerprint" accompanies the fish on every step of its journey – from the dock to the factory, on to the wholesaler and retailer – where it



is registered and updated before being passed on to the next link in the supply chain. In the end, the consumer can scan a QR code to trace the information back to the catch and thus know for certain what has landed on the dinner table. The entire procedure could be further improved by combining the blockchain with smart contracts and the Internet of Things: for instance, sensors could monitor whether the prescribed temperature is maintained during transport and ensure that transported goods are not manipulated; if necessary, the sensors trigger a predefined response. All these steps help to ensure product quality.

Although monitoring and securing supply chains is also possible without blockchain technology, blockchain-based networks optimise the tracking of goods and ensure correct procedures. Nevertheless, error cannot be excluded: in the case of tuna fishing, the authority charged with controlling and assuring compliance with sustainability criteria could be negligent. Trust in a system's guarantors therefore remains a necessary component; in this scenario, however, the blockchain is not a fully "trust-less" system – one in which trust in intermediaries is completely replaced by a decentralised public and transparent network.

Smart energy management – the sun over Brooklyn

The previous examples show that the blockchain's strengths are currently best suited for scenarios in which the technology fills a gap. This specifically applies to settings where trust – the basis of every transaction – is lacking or difficult to create because no centralised authority exists or because too many error-prone intermediaries are involved. Whether it is a national register, shopping in a refugee camp or precisely tracking the delivery route of responsibly fished tuna: in all these applications, the blockchain functions more as a supplementary feature in existing analogue or digital networks. Indeed, blockchain-based tools are often only convincing when they are limited to a local setting. One such example is found on the roofs of Brooklyn.

In the Park Slope neighbourhood of Brooklyn, New York, a group of neighbours living in a row of brownstone townhouses joined forces to create a decentralised micro energy grid. The collective is producing solar energy for their personal use, but they also want to feed surplus electricity into the grid at a fair price. Moreover, they want to be able to say which electricity prices they are prepared to pay should they themselves need to tap into their neighbours' grid. "Brooklyn Microgrid" is the name of the successful project that uses a combination of a private blockchain platform and smart contracts to distribute energy according to supply and demand. Prices are set in automated auctions via smart contracts; they are based on the highest price that a consumer participating on the microgrid is prepared to pay and on the lowest price at which an energy company is willing to sell. The platform comprises control systems, converters, smart meters and energy storage devices in the form of lithium-ion batteries. In this system, electricity is traded and charged directly between producers and consumers; an intermediary utility provider is unnecessary. The Brooklyn Microgrid is, however, not entirely decoupled from the energy grid and, if necessary, the Microgrid participants can procure electricity from the public utility.

Lawfully implementing similar projects in Switzerland and, for instance, supplying entire cities with electricity via a public, decentralised peer-to-peer platform in which energy companies do not act as intermediaries would first require a restructuring of today's energy market. Under the prevailing rules and regulations in the energy sector, such projects are impossible: Switzerland's not yet completely deregulated energy market currently prevents small-scale energy consumers from participating in the market. Moreover, the costs for using the grid are strictly regulated and cannot be lowered when electricity is generated locally.

The hunt for a killer application

To date, no application has been created that makes the blockchain indispensable: tried and tested alternatives for most blockchain applications already exist, and many innovative uses of the blockchain would be just as interesting without blockchain technology. This condition, however, has less to do with the technology itself than with the fact that the blockchain in its purest form as a decentralised, public, entirely transparent and trusted database is a drastic departure from existing legal and regulatory measures. As such, it calls into question existing economic and business structures as well as a great many private and national institutions.

The blockchain as a catalyst

Although actual blockchain applications are at present of marginal importance, the technology's significance as a social phenomenon is not to be discounted. Highly complex and largely incomprehensible to the layperson, the blockchain has become a surface for projections that various interest groups with differing motives busily polish, especially in the area of cryptocurrencies. One example is provided by the so-called "White Papers": articles that are often published in cryptic tech parlance and used to launch ICOs. These White Papers often more closely resemble a marketing campaign than a tool to provide potential investors with solid information – and they also are most likely intended to conceal a product's actual value for end-users while also pre-emptively evading responsibility for technical problems.

Trust, control, accountability

Conceived from the start as a libertarian alternative to a world in which nation-states function as centralised oversight authorities, the blockchain is not only situated outside accepted regulatory and legal measures in numerous sectors, but it also calls into question a wide range of societal and political values. Proponents of the blockchain frequently dream of doing away with governmental and market-driven structures in the hope that a blockchain-based, decentralised world order could bring about greater efficiency and fairness.

As such, trust in a supervisory authority that guarantees correctness in all procedures is replaced with trust in a complex cryptographic system and an oversight mechanism that is based on consensus among all participants. The probability that errors should occur on the blockchain is held to be negligible; nevertheless, should the system malfunction, no entity could be held accountable.

Transparency versus privacy

The blockchain's main strength is its absolute transparency – for instance, enhancing food safety by meticulously documenting each step of a delivery chain. The price of this transparency is, however, that the identity and the privacy of users are not adequately protected. A participant who owns the public key of a user can track that specific user's transactions, then compare and link transaction patterns with other data sets – and thus potentially discover the identity of the individual behind a pseudonym. Because the blockchain is designed to store data in a way that makes information undeletable and safe from manipulation, the right to be forgotten is not given.

Taming the tiger – but as a collective

The fact that the blockchain functions without trusted intermediaries represents a challenge to all institutions that have previously taken on this role and casts doubt on their justification. Cryptocurrencies in particular have been targeted by regulatory bodies across the globe, and many countries have already forbidden them. Another option is the use of "regulatory sandboxes" to create soft pressure and steer cryptocurrencies into more regular channels without, however, endangering innovation. Currently, the World Wide Web Consortium is developing international standards that clarify contexts for using blockchain applications.

Apart from regulatory measures and standards, other tools to tame the blockchain are also being considered: in finance and industry, big names have long begun to transform the technology that is threatening their traditional business models into something that serves their own purposes. This has led to the development of private blockchains with restrictions on who can participate; in the meantime, these private networks have also been adopted by many governmental bodies. Some countries are even considering launching a national cryptocurrency.

It is important that attempts to normalise the technology are not dominated by interests, desires and fears of participants that have no democratic legitimation. To serve the interest of the general public, the ways of using a highly innovative technology that calls into question so many existing structures must – far removed from the hype – be deliberated in broad-based, pragmatic discussions. This is the goal that TA-SWISS has pursued in compiling and presenting the two-part report at hand.

Supervisory Group

- Dr. Olivier Glassey, head of the supervisory group and member of the TA-SWISS Steering committee, University of Lausanne
- Raphael Bucher, Federal Office for the Environment (FOEN)
- Prof. Christian Cachin, University of Bern
- Hannes Gassert, crstl
- Anja Wyden Guelpa, civiclab
- Dr. Uwe Heck, Federal IT Steering Unit (FITSU)
- Luzius Meisser, meissereconomics
- Marine Pasquier-Beaud, Swiss Federal Office of Energy (SFOE)
- Martin Rindlisbacher, UBS
- Dr. Fabian Schnell, Avenir Suisse
- Antoine Verdon, Swiss Legal Tech Association

Project management at TA-SWISS

- Dr. rer. soc. Elisabeth Ehrensperger, Managing director
- Dr. Catherine Pugin, Project manager

Impressum

Programmed trust:
Opportunities and risks of blockchain technology
Summary of the study «Blockchain: Capabilities, Economic Viability, and the Socio-Technical Environment»
TA-SWISS, Bern 2020
TA 73A/2020

Author: Christine D’Anna-Huber, Wissenschaft im Text, Paradiso
Translation: Pro-Verbial, Zürich
Production: Fabian Schluep, TA-SWISS, Bern
Layout and graphics: Hannes Saxer, Bern
Printed by: Jordi AG – Das Medienhaus, Belp

TA-SWISS – Foundation for Technology Assessment

New technology often leads to decisive improvements in the quality of our lives. At the same time, however, it involves new types of risks whose consequences are not always predictable. The Foundation for Technology Assessment TA-SWISS examines the potential advantages and risks of new technological developments in the fields of life sciences and medicine, information society as well as mobility, energy and climate. The studies carried out by the Foundation are aimed at the decision-making bodies in politics and the economy, as well as at the general public. In addition, TA-SWISS promotes the exchange of information and opinions between specialists in science, economics and politics and the public at large through participatory processes. Studies conducted and commissioned by the Foundation are aimed at providing objective, independent, and broad-based information on the advantages and risks of new technologies. To this purpose the studies are conducted in collaboration with groups comprised of experts in the relevant fields. The professional expertise of the supervisory groups covers a broad range of aspects of the issue under study.

The Foundation TA-SWISS is a centre for excellence of the Swiss Academies of Arts and Sciences.

TA-SWISS
Foundation for Technology Assessment
Brunngasse 36
CH-3011 Bern
info@ta-swiss.ch
www.ta-swiss.ch

member of the
swiss academies
of arts and sciences