



Grant Agreement No.: 101102718 Call: DIGITAL-2022-DEPLOY-02

Type of action: DIGITAL-CSA



SEEBLOCKS.eu

Supporting Europe's effort in Blockchain/DLT Standardisation

D3.1 Blockchain and DLT standardisation landscape report

Work package	WP3 "Pan-European and international synergies"
Task	T3.2
Due date	31/08/2023
Submission date	31/08/2023
Deliverable lead	DCU
Version	V1.0 DRAFT NOT YET APPROVED BY THE EUROPEAN COMMISSION
Authors	Fiona Delaney (DCU)
Reviewers	Sharon Farrell (DCU), John Favaro (Trust-IT)
Keywords	Landscape Report, Open Standards, Terminology

Document Revision History

Version	Date	Description of change	List of contributors
0.1	20.08.2023	Table of Contents, Introduction, Sections 1-3	Fiona Delaney (DCU)
0.2	22.08.2023	Section: Focus on Europe	Sharon Farrell (DCU), Fiona Delaney (DCU)
0.3	24.08.2023	Final draft	Sharon Farrell (DCU), Fiona Delaney (DCU)
0.4	24.08.2023	Peer-review and formatting	John Favaro (Trust-IT)
1.0	28.08.2023	Final quality check	John Favaro (Trust-IT)

Disclaimer

SEEBLOCKS.eu has received funding from the European Union's Digital Europe Programme under Grant Agreement No. 101102718. The content of this document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

Dissemination Level		
PU	Public, fully open, e.g., web	✓
CO	Confidential, only for members of the consortium (including the Commission)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	EU-SEC. Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

* *R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

Executive Summary

SEEBLOCKS.eu supports EU strategic autonomy with standardisation. This document, the first in a series of Landscape Reports to be released throughout the term of the project, provides an overview of the current status of blockchain and DLT technology in Europe and globally, and details efforts supporting digital innovation and EU autonomy through a standardisation lens. It also outlines the process of creating open standards for blockchain and distributed ledger technology (DLT), and provides a selection of important published standards from international bodies. It is organised as follows.

1. Focus on Blockchain in Europe

Europe's focus on blockchain technology is evident through initiatives like the European Blockchain Partnership, the European Blockchain Services Infrastructure, and new EU Crypto Markets and Virtual Assets regulations. These efforts aim to achieve digital autonomy, standardisation, and financial regulation.

2. How Are Open Standards Made?

This section explains the collaborative process behind creating open standards for blockchain and DLT. The creation of open standards is a collaborative process involving cooperation, consensus, and industry participation. Research excellence, and the involvement of Standards Development Organisations (SDOs) and industry representative bodies are key components of this process.

3. Blockchain and DLT Standards

Published standards and upcoming work items are crucial for ensuring interoperability and alignment across different sectors, this section presents some key standards both published and in the pipeline that accelerate impact.

4. Conclusion

Blockchain and DLT standards play a pivotal role in enhancing transparency, trust, and interoperability across industries, contributing to the growth of the digital economy. SEEBLOCKS aims to play a significant role in supporting standards and innovation.

Table of Contents

Executive Summary	4
Table of Contents	5
List of Figures	6
List of Tables	6
Abbreviations	7
1. Introduction	9
1.1 Focus on Blockchain in Europe	9
1.2 Digital Autonomy	10
1.3 EU Standardisation Rolling Plan	10
1.4 EU Blockchain Sandbox	10
1.5 EU Financial Regulation	11
2. How are open standards made?	12
2.1 SDOs, SSOs, industry and national bodies	12
2.2 Cooperation, consensus, and requests for comment	13
3. Blockchain and DLT standards	17
3.1 Examples of published standards (SDOs and SSOs)	18
3.2 Examples of pre-publication new work items	21
3.3 Examples of transversal standards	21
4. Conclusion	22

List of Figures

Figure 1: Breakdown of published, emerging, and transversal standards 18

List of Tables

Table 1: ISO standardisation principles and two examples of emerging DLT standards 15

Table 2: EIPs and ERC standards 16

Table 3: Published Blockchain and DLT standards ISO, IEC, ITU 20

Table 4: Pre-publication new work items from ISO, IEC, ITU 21

Table 5: Transversal standards from ISO, IEC, ITU 21

Abbreviations

Acronym	Description
AML	Anti Money Laundering
API	Application programming interface
AWI	Approved work item
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht
CD	Committee draft
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
DID	Decentralised Identifier
DLT	Distributed Ledger Technologies
DAO	Decentralized autonomous organization
EBP	European Blockchain Partnership
EBSI	European Blockchain Services Infrastructure
EC	European Commission
EIP	Ethereum Improvement Proposal
ERC	Ethereum Request for Comment
ETSI	European Telecommunications Standards Institute
EU	European Union
eWpG	Gesetz zur Einführung elektronischer Wertpapiere
FACR	Financial and Administrative Coordinator Representative
FATF	The Financial Action Task Force
FG	Focus group
HTTP	Hyper Text Transfer Protocol
INATBA	International Association for Trusted Blockchain Applications
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
ISMS	Information security management system
ISO	International Standards Organisation
ITU	International Telecommunication Union
JWG	Joint working group
KWG	Kreditwesengesetz
MiCA	Markets in Crypto Assets
MiFID	Markets in Financial Instruments Directive

NB	National (standards) body
NC	National committee
NFT	Non-fungible token
NSB	National Standard Bodies
OID	Object identifier
PWI	Proposed work item
RFC	Request for comment
SDO	Standard development organisation
TC	Technical committee
TR	Technical report
TS	Technical specification
URI	Universal resource identifier
VASP	Virtual asset service provider
WD	Working draft
WG	Working group
WSC	World Standards Cooperation

1. Introduction

The emerging role of blockchain and DLT in the economy enhances transparency and trust in business, trade and operations. This role brings optimised visibility for both subjects and objects of trade (including digital and virtual assets) that are represented in a system and under agreement in a multi-party system. Such systems are designed to enable collective, cooperative, consortium and/or federated business process handling in online and virtual contexts.

SEEBLOCKS.eu has a mission to accelerate interoperability, transversal alignment, preparedness and resilience in the single digital marketplace. It does this by connecting open standards experts and research in a targeted two-year program to advance blockchain and distributed ledger technology (DLT) open standards. SEEBLOCKS.eu recognises that the European single marketplace is a significant trading partner in the global digital economy and the resilience and preparedness required shall be outward-facing as well as to inwards-facing. To this end, an open innovation strategic approach guides the project.

Trade in the global digital marketplace has evolved and products and services have become bundled with various metadata, access and intellectual property rights. Blockchains and DLTs add functionality to long-standing trade facilitation concepts such as trust anchors and registries, and facilitate a simple binding of valuable rights to locations, entities and artifacts that emerge post-digitalisation – e.g., digital twin, metaverse, and generative adaptations of humanity (imagination, image, voice, body).

Technical interoperability and transversal alignment are key aspects of industry preparedness and resilience, these can be achieved through open standards development and open source resources.

1.1 Focus on Blockchain in Europe

The [European Blockchain Partnership](#) (EBP) was created in April 2018 by a Joint Declaration and includes all EU Member States and members of the European Economic Area (Norway and Liechtenstein). The signatories of this Joint Declaration commit to working together towards realising the potential of blockchain-based services for the benefit of citizens, society and the economy.

As part of this commitment, the Partnership established the [European Blockchain Services Infrastructure](#) (EBSI), to deliver EU-wide cross-border public services using blockchain technology. EBSI is guided by an open innovation approach to research and knowledge transfer, encouraging early adoptive public sector bodies to experiment with harmonised public sector digitalisation strategies across the single digital marketplace. This approach focuses on common use cases including: verified credentials, self-sovereign identity management, wallet security and many more.

Additionally, though largely out of scope of the EPB, the European Commission, as with many other governments and regional trade entities, has placed a watchful eye on the emergence of digital and cryptocurrencies, tokens and virtual assets.

Financial regulators the world over seek to strike a balance between limiting growth and risking devaluation, capital flight and other destabilising influences in their economies due to the emergence of new digital fungible and non-fungible stores of value and means of exchange.

1.2 Digital Autonomy

The European [Blockchain strategy](#) (2021) is recognised in the [Europe's Digital Decade and autonomy](#) report as designed to enable innovation, accelerate the adoption of blockchain technologies, and create a balanced and consistent legal framework for blockchain technology and digital assets. The instruments for this enablement include the EBP and EBSI which currently promotes the first public sector blockchain services in Europe.

The problem relating to EU digital autonomy was initially defined as centring on digitalisation – the transition from paper to digital – and how to share official documents and exchange credentials in a trusted way. Could blockchain facilitate a change to a decentralised exchange protocol, supporting the verification of entities and the authenticity of information without requiring real-time access to the source of the information?

Subsequently, considerations grew to include a more detailed analysis of the legal and regulatory implications, leading to the establishment of the [EU Blockchain Sandbox](#) (2022) and a more refined scoping of specific industry requirements (health, food, energy and financial services including new crypto-facing financial regulations) and transversal standardisation requirements in the [EU Standardisation Rolling Plan](#) (2023 version).

1.3 EU Standardisation Rolling Plan

The objective of the [EU Standardisation Rolling Plan](#) is to bridge the gap between EU policies and standardisation activities. In the case of Blockchain/DLT their role is to support the Rolling Plan specifically in regards to the topic of Blockchain and DLT. The FinTech industry has already engaged with Blockchain/DLT, but this needs to be further developed into the different sectors. It also must bridge the gap and cement the relationship with the EBP and support the participation of the EBSI.

In 2020 the EU organised a webinar '[Joining Forces for Blockchain Standardisation](#)' to generate good collaboration and cohesion of standardisation activities. It brought together a number of Blockchain standards experts, who discussed standardisation of Identity, Interoperability, Governance, and Smart Contracts. It was acknowledged in this webinar that more cohesion is needed in most critical areas of blockchain standardisation. It was concluded that “interoperability” would benefit the most, followed by “identity”, “smart contracts”, “governance”, and “security”.

1.4 EU Blockchain Sandbox

In February 2023, Europe launched the [EU Blockchain Sandbox](#) environment. This provides a safe and secure environment for the testing of Blockchain. The sandbox will give support to the testing of Blockchain, ensuring assistance with the risks and issues surrounding the testing of Blockchains.

The sandbox will run for three years (2023 to 2026), and is forecasted to support 20 projects annually. This will include public sector uses cases from the EBSI, including public sector use

cases on the European Blockchain Services Infrastructure (EBSI) – a [multi-country project](#) under the Digital Decade supported by the Commission, all Member States, Norway, and Liechtenstein. The [first call](#) opened on 14 April 2023.

Follow this [link](#) to know more about 'How to get connected to the EU Blockchain Sandbox'.

1.5 EU Financial Regulation

Recent approaches to financial services regulation are marked by efforts to classify and regulate crypto assets.

In Europe, the Markets in Crypto Assets Regulation (MiCA) establishes a regulatory framework for virtual asset issuers and service providers similar to financial instruments under the Markets in Financial Instruments Directive (MiFID, 2014). MiCA aims to ensure legal certainty, investor protection, and financial stability for various types of crypto assets.

Germany has taken a proactive approach by including crypto assets in its Banking Act (*Kreditwesengesetz* or KWG) and introducing regulations for tokenised traditional financial instruments. The KWG includes crypto assets/units of account as non-MiFID financial instruments and adds custody of crypto assets as a financial service requiring a license from the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* or BaFin).

The Electronic Security Act (*Gesetz zur Einführung elektronischer Wertpapiere* or eWpG) concerns the tokenisation of traditional financial instruments. The eWpG introduces a 'crypto securities registrar', an entity responsible for maintaining a decentralised register for authorised instruments issued on a distributed ledger technology.

Efforts are being made globally to address anti-money laundering and combat financing of terrorism concerns. The Financial Action Task Force (FATF) has made recommendations for regulating virtual asset service providers (VASPs), influencing jurisdictions including the EU, Hong Kong, Singapore, and Australia to implement AML/CFT rules for VASPs.

Overall, the increasing prominence of crypto assets in the financial landscape has prompted regulators worldwide to seek clarity and greater insights directly from those financial service providers in the ecosystem.

2. How are open standards made?

To achieve the SEEBLOCKS objective of accelerating technical interoperability, transverse sectoral alignment, preparedness and resilience in the global digital marketplace, a common view of open standards, relevant actors, organisations and methods is key.

In this section we review diverse processes by which open standards are proposed, refined and agreed; by whom, when and where.

2.1 SDOs, SSOs, industry and national bodies

Standards organisations can be classified by geography (e.g., international, regional, national), and/or by industry section (e.g., technology, finance, agriculture).

An SDO is a *standards developing organisation*, and an SSO is a *standards setting organisation* (SSO). SDOs and SSOs may be national, regional or international in remit and develop industry specific standards, guidance and specifications to promote business, legal and technical interoperability.

International standards development organisations (SDOs)

International SDOs develop international standards. International standards are largely voluntary and do not restrict the use of other standards or none. The three largest SDOs, named below, have over time established processes for developing and publishing voluntary international standards.

- International Organisation for Standardisation (ISO), established in 1947, a private organisation, comprised of a single national standards body (NB) per nation state.
- International Electrotechnical Commission (IEC), established in 1906, a private organisation, comprised of a single national committee (NC) per nation state.
- International Telecommunication Union (ITU), established in 1865, established by treaty as a permanent agency of the United Nations.

Together, they comprise the World Standards Cooperation (WSC) alliance, formed in 2001. The WSC promotes a voluntary consensus-based International Standards system and is an example of an SSO.

Regional standards organisations

Three important regional standards bodies in Europe are:

- European Committee for Standardization (CEN)
- European Committee for Electrotechnical Standardization (CENELEC)
- European Telecommunications Standards Institute (ETSI)

In the European Union, per Regulation (EU) No 1025/2012 only standards created by CEN, CENELEC, and ETSI are recognised as European standards. Member states shall notify the European Commission and each other about all draft technical regulations for ICT products and services before they are adopted in national law per Directive 98/34/EC to enhance transparency and control within the single digital marketplace.

2.2 Cooperation, consensus, and requests for comment

Open standards generally arise through the Socratic method of dialogue. Proposals are first shared or broadcast, considered and discussed (frequently at length) and ultimately concluded by a process of consensus and acceptance.

Depending on the context, a new standard might be adopted, applied, or published. In this section we explore common methods of cooperation that achieve excellence in standards development, and give examples from the recent history in blockchain and DLT.

Consensus-based cooperation

ISO standards are created for and by those who use them. They are developed in a multi-stakeholder review and comment process and gain approval through a structured consensus and ballot lifecycle.

Table 1 outlines four key principles of standard development at ISO and highlights two examples, one published and one at the beginning of its lifecycle, that demonstrate the breadth of ISO standardisation activities in relation to DLTs.

International Standards Organisation (ISO)			
Key principles in ISO standard development Source .			
<i>Respond to a need in the market</i>	<i>Based on global expert opinion</i>	<i>Developed through a multi-stakeholder process</i>	<i>Based on a consensus</i>
A request for a new standard is made. Typically, an industry sector or group communicates the need for a standard to its national body	ISO standards are developed by groups of experts from all over the world, whose participation is mediated through ISO technical committees. These experts negotiate all aspects of	Technical committees are made up of experts from the relevant industry, but also from consumer associations, academia, NGOs and government.	Developing ISO standards is consensus-based and comments from all stakeholders are taken into account.

member who contacts ISO.	the standard, including its scope, key definitions and content.		
Ex. 1	ISO/TS 23635:2022 Blockchain and distributed ledger technologies — Guidelines for governance. Source .		
<p>ISO/TS 23635:2022 is a standard proposed by experts at ISO TC307 WG 5 Governance, who recognised that for organisations and broader industries, it is difficult to engage in the development of DLT systems in the absence of effective DLT-governance mechanisms.</p> <p>In the case of permissionless public distributed ledgers, they can comprise an unrestricted number of potentially pseudonymous DLT users and nodes. In permissioned public blockchains they can have hybrid governance structures.</p> <p>In the absence of a central governing authority, several governance questions regarding ownership, decision rights, responsibilities and accountabilities, and incentive structures emerge that cannot be addressed by applying traditional mechanisms.</p> <p>This standard is at stage 60.60 and was published in 2022.</p> <p>ISO/TS 23635:2022 Blockchain and distributed ledger technologies — Guidelines for governance provides guiding principles and a framework for the governance of DLT systems. The document also provides guidance on the fulfilment of governance, including risk and regulatory contexts, that supports the effective, efficient, and acceptable use of DLT systems.</p>			
Ex. 2	Proposed Work Item 23095 - 27002 for distributed ledger services. Source .		
<p>PWI 23095 is a proposal to pursue an extension to the internationally recognised cybersecurity standard ISO/IEC 27002:2002 for DLT applications and services. It is proposed by experts at ISO TC307 JWG4 Security, privacy and identity for Blockchain and DLT. The proposal is at stage 0.0.</p> <p>ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls provides a reference set of generic information security controls including implementation guidance. It is designed to be used by organizations: a) within the context of an information security management system (ISMS) based on ISO/IEC27001; b) for implementing</p>			

information security controls based on internationally recognized best practices; c) for developing organization-specific information security management guidelines.

Table 1: ISO standardisation principles and two examples of emerging DLT standards

Improvement Proposals and Requests for Comment

Protocol standards, such as those governing the internet or other decentralised infrastructure, have a less conclusive, though similarly discursive process that may lead to a rough consensus. One example is the original proposal for the now-ubiquitous HTTP protocol (1996) documented on the Internet Engineering Task Force (IETF) data tracker archive. RFC-1945 was contributed by Neilson, Fielding and Berners-Lee. It is in essence a protocol proposal, which “provides information for the Internet community” and “does not specify an Internet standard of any kind.” Despite the disclaimer, the Memo is flagged by the Internet Engineering Steering Group (IESG) “The IESG has concerns about this protocol, and expects this document to be replaced relatively soon by a standards track document”, thereby demonstrating that proposals are monitored and guided toward appropriate tracks for consideration.

In relation to DLT-based improvements, developing standards by agreement is also part of the process: Ethereum Improvement Proposals (EIP) and Requests for Comments (RFC) processes. An EIP is the improvement proposal process for any changes to the Ethereum environment, protocol and token standards. Unlike at ISO, the proposer is responsible for building consensus within the community and documenting dissenting opinions.

Ethereum Requests for Comment (ERCs) describe novel application-level conventions that affect most (or all) existing Ethereum implementations, including contract standards such as token standards (ERC-20 fungible token, ERC-720 non-fungible token standards), name registries (ERC-137), URI schemes, library/package formats, and wallet formats. Table 2 includes further detail on EIPs and ERCs, and highlights two examples, one final and one currently under review to demonstrate the method of standards acceptance at the Ethereum organisation.

Ethereum.org		
Ethereum Improvement Proposals and Requests for Comment		
<i>What are EIPs?</i>	<i>EIP repository</i>	<i>Types of EIPs</i>
EIPs are the primary mechanisms for proposing new features, for collecting community technical input on an issue, and for	EIPs are maintained as text files in a versioned repository. Their revision history is the historical record of the feature proposal.	Standard, Meta and Informational. Standards track EIPs can be further categorised as Core, Networking, Interface and ERC. They consist of three parts—a design document, an implementation, and

documenting design decisions.		(if warranted) an update to the formal specification.
Ex. 1	ERC-1155 MULTI-TOKEN STANDARD [Final] Source	
<p>ERC-1155 standard outlines a smart contract interface that can represent any number of fungible and non-fungible token types. Existing standards such as ERC-20 require deployment of separate contracts per token type. The ERC-721 standard's token ID is a single non-fungible index and the group of these non-fungibles is deployed as a single contract with settings for the entire collection. In contrast, the ERC-1155 Multi Token Standard allows for each token ID to represent a new configurable token type, which may have its own metadata, supply and other attributes.</p>		
Ex. 2	ERC-5725 Transferable Vesting NFT [Under Review] Source	
<p>A Non-Fungible Token (NFT) standard used to vest ERC-20 tokens over a vesting release curve. The standard allows for the implementation of a standard API for NFT based contracts which represent the vested and locked properties of underlying ERC-20 tokens that are emitted to respective NFT owners.</p> <p>This standard is an extension of the ERC-721 token which provides basic functionality for creating vesting NFTs, claiming underlying tokens and reading vesting curve properties.</p>		

Table 2: EIPs and ERC standards

3. Blockchain and DLT standards

For the purpose of achieving SEEBLOCKS objectives, the following set of **Priority areas** (far left column in the tables in this section) for Blockchain and DLT have been selected along with foundational standards. In addition to foundational aspects (e.g., vocabulary, taxonomy, and ontology), a number of blockchain and DLT specific focus areas emerge including:

1. **Identity management** (e.g., self-sovereignty; privacy; anonymity; account abstraction; secure wallet management);
2. **Data provenance** (e.g., on/off-chain data flows; data trustworthiness; verifiable oracle services/registries);
3. **Governance** (e.g., stakeholder reputation including roles, rights and responsibilities; online voting; DAOs; peer-to-peer virtual communities);
4. **Token and asset creation and exchange** (e.g., cryptocurrency; virtual assets; fungible and non-fungible tokens; exchange protocols);
5. **Process optimisation** (e.g., process transparency; multi-party, interoperable, cloud-based resource-sharing; 5G and mobile edge computing; energy-efficiency);
6. **Automation** (e.g., smart contracts; intelligent agency; robotics);
7. **Cybersecurity and applied game theory** (e.g., open source, distributed and decentralised system architectures; end-point security; encryption; consensus mechanisms);
8. Use cases that elaborate these niches or other relevant domains.

Of the standards itemised in the following sub-sections we can see a spread across Priority Areas in Figure 1, which shows a breakdown of published, emerging and transversal standards listed in this document (August 2023) and categorised per SEEBLOCKS priority area analysis.

SEEBLOCKS standards landscape analysis

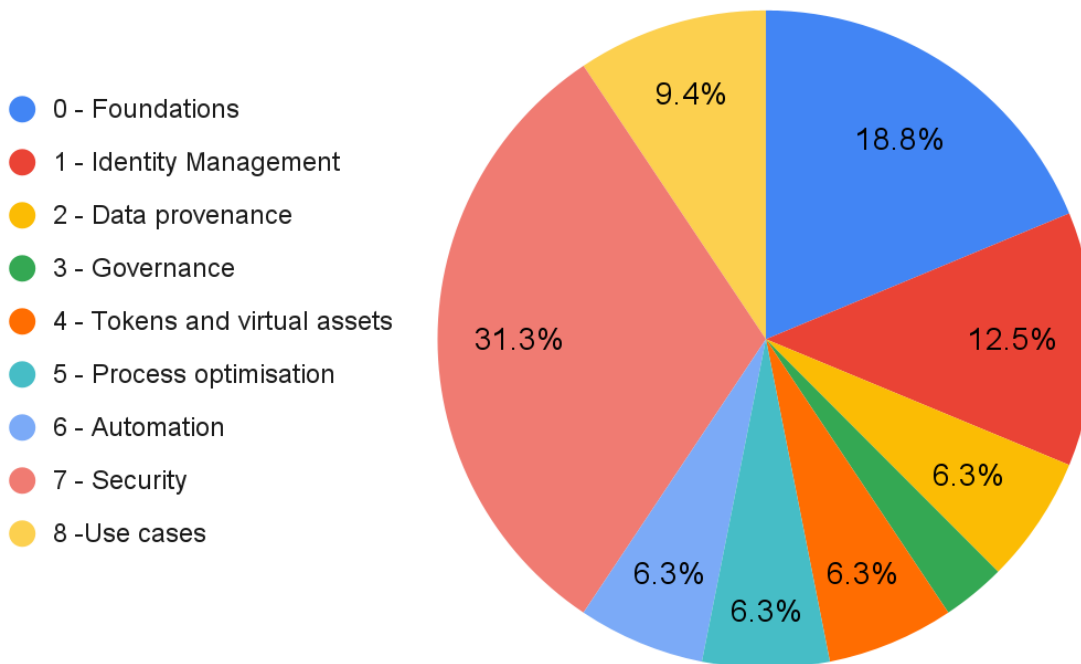


Figure 1: Breakdown of published, emerging, and transversal standards

3.1 Examples of published standards (SDOs and SSOs)

Table 3 contains a representative list of Blockchain and DLT standards published by ISO, IEC, and ITU.

Priority area	Title	Link	Year
ISO	ISO TC307 Blockchain and DLT	TC307	2016
Technical Specifications			
3	Blockchain and DLT - Guidelines for governance	ISO/TS 23635:2022	2022
7	Blockchain and DLT - Reference architecture	ISO/TS 23257:2022	2022

0	Blockchain and DLT - Taxonomy and Ontology	ISO/TS 23258:2021	2021
0	Blockchain and DLT - Vocabulary	ISO/TS 22739:2020	2020
Technical Reports			
1	Blockchain and DLT - Overview of trust anchors for DLT-based identity management	ISO/TR 23644:2023	2023
1	Blockchain and DLT - Identifiers of subjects and objects for the design of blockchain systems	ISO/TR 6039:2023	2023
1	Blockchain and DLT - Overview of existing DLT systems for identity management	ISO/TR 23249:2022	2022
8	Blockchain and DLT - Use cases	ISO/TR 3242:2022	2022
1	Blockchain and DLT - Privacy and personally identifiable information protection considerations	ISO/TR 23244:2020	2020
4	Blockchain and DLT - Security management of digital asset custodians	ISO/TR 23576:2020	2020
6	Blockchain and DLT - Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems	ISO/TR 23455:2019	2019
ITU			
ITU	Focus Group on Application of DLT	FG DLT	2017
Priority area	Title	Id and link	Year
7	Security framework for data access and sharing management system based on distributed ledger technology	T17-SG17-210824--TD-PLN-4017	2021
7	Security guidelines for using DLT for decentralized identity management	T17-SG17-200824--TD-PLN-3371	2020
7	Security assurance for distributed ledger technology	T17-SG17-200824-TD-	2020

		PLEN-3294	
7	Security threats to Distributed Ledger Technology	T17-SG17-190827-TD- PLEN-2441	2019
7	Security framework for distributed ledger technology	T17-SG17-200317-TD- PLEN-2831	2920
7	Security requirements for digital integrity proofing service based on distributed ledger technology	T17-SG17-220107-TD- PLEN-4211	2022
7	Security services based on distributed ledger technology	T17-SG17-210824-TD- PLEN-4012	2021
7	Security threats to online voting system using distributed ledger technology	T17-SG17-210420-TD- PLEN-3650	2021
0	Requirements for distributed ledger systems	T17-SG16-200622-TD- PLEN-0436	2020
0	Assessment criteria for distributed ledger technologies	T17-SG16-200622-TD- PLEN-0437	2020
0	Reference framework for distributed ledger technologies	T17-SG16-200622-TD- PLEN-0451	2020

Table 3: Published Blockchain and DLT standards ISO, IEC, ITU

3.2 Examples of pre-publication new work items

Table 4 contains a set of examples of ISO, IEC, and ITU pre-public new work items.

Priority Area	Title	Link	status
ISO	ISO TC307 Blockchain and DLT	TC307	2016
5	Blockchain and DLT - Interoperability Framework	ISO/AWI TS 23516	20.00
8	Blockchain and DLT - Data flow model for blockchain and DLT use cases	ISO/CD TR 6277	50.20
4	Blockchain and DLT - Representing Physical Assets using Non-Fungible Tokens	ISO/AWI 20435	20.00
6	Blockchain and DLT - Overview of smart contract security good practice and issues	ISO/WD TR 23642	20.00

Table 4: Pre-publication new work items from ISO, IEC, ITU

3.3 Examples of transversal standards

Table 5 contains a set of examples of transversal standards elaborated by ISO, IEC, and ITU.

Priority Area	Title	Link	Year
2	Application of blockchain-based traceability platform for cold chain food	ISO/TR 16340:2023	2023
7	Information security, cybersecurity and privacy protection — Information security controls	ISO/IEC 27002:2022	2022
8	Internet of Things (IoT) - Integration of IoT and DLT/blockchain: Use cases	ISO/IEC TR 30176:2021	2021
5	OID-based resolution framework for transaction of distributed ledger assigned to IoT resources	T17-SG20-201106-TD-GEN-1948	2020
5	Reference architecture of blockchain-based unified KPI data management for smart sustainable cities	T17-SG20-200706-TD-GEN-1792	2020
0	Digital evidence services based on distributed ledger technology	T17-SG16-190319-TD-WP2-0173	2019

Table 5: Transversal standards from ISO, IEC, ITU

4. Conclusion

Distributed ledger technologies offer a robust layer in emerging industry contexts where value derives from prodigious mineable data resources, from the tangible context of trade finance and eCommerce supply chains, to the increasingly intangible contexts of industry 4.0 (e.g., agri-food integrity, smart energy microgrid reconciliation, Net Zero reporting).

Disruptive and less-established markets in entirely-virtualised experiences (e.g., online gaming, metaverse and digitalised performances for online consumer communities) are also on the rise. It is anticipated that blockchain and DLT have a role to play in bringing a foundation layer of trust and transparency in these contexts, too.

The impact of the contributions is just as unknowable as the impact of the original [‘Bitcoin P2P eCash paper’](#) was when it was posted on the Cryptography noticeboard on November 1, 2008.

SEEBLOCKS efforts in providing support and expert guidance to those active contributors in open standards development are expected to yield measurable impact on the ecosystem and bring robust benefits to the European community and beyond.