



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

Type of action: DIGITAL-CSA



**SEEBLOCKS.eu**  
Supporting Europe's effort in Blockchain/DLT Standardisation

## D3.6 Landscape & Gap Analysis Report on Blockchain/DLT Standardisation - Final

Work package	WP3 “Pan-European and international synergies”
Task	T3.3
Due date	31/05/25
Submission date	29 <sup>th</sup> May 2025
Deliverable lead	DCU
Version	V1.0 <b>DRAFT NOT YET APPROVED BY THE EUROPEAN COMMISSION</b>
Authors	Mohammad Fardad, Maryam Basereh, Irina Tal, Sharon Farrell
Reviewers	FhG (Knut Blind)
Keywords	Landscape Report, Open Standards, Terminology

## Document Revision History

Version	Date	Description of change	List of contributors
0.1	01/04/25	Table of Contents, Structure agreed	Mohammad Fardad, Irina Tal
0.2	21/04/25	Section 1: Introduction	Mohammad Fardad, Maryam Basereh
0.3	05/05/25	Section 2, 3, 4	Mohammad Fardad, Maryam Basereh, Irina Tal
0.4	09/05/25	Review and updates	Irina Tal
0.5	20/05/25	Review and updates following TWG feedback	Mohammad Fardad, Maryam Basereh, Irina
0.6	21/05/25	Peer-review	Knut Blind
0.7	23/05/25	Updates following review	Mohammad Fardad, Maryam Basereh, Irina Tal
0.8	26/5/25	Formatting after review	Sharon Farell
1.0	29/05/25	Final quality check	Rita Meneses

## 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

The **SEEBLOCKS D3.6 Landscape and Gap Analysis Report on Blockchain/DLT Standardisation** is the last in a series of SEEBLOCKS reports on this topic and presents a comprehensive assessment of the current blockchain and distributed ledger technologies (DLT) standardisation ecosystem, identifying existing gaps, while also highlighting targeted SEEBLOCKS responses to some of these gaps and proposing recommendations.

### Key Findings

- **Expanded Standards Landscape** The report catalogs **116 blockchain/DLT-related standards**, reflecting growing international efforts to harmonize technical, governance, and interoperability frameworks. These standards span multiple domains, including identity, smart contracts, data provenance, cybersecurity, governance, and automation.
- **Identified Standardisation Gaps** Persistent gaps were identified in key areas such as:
  - a. **Consensus mechanisms** (lack of detailed, adaptable standards);
  - b. **Interoperability** (limited cross-platform, tech-neutral frameworks);
  - c. **Permission models** (no dedicated standards for access control in DLT environments)  
Additional priority areas include smart contracts, provenance, governance, and record management.
- **Alignment with EU Rolling Plan** The analysis aligns with the **EU Rolling Plan for ICT Standardisation**, emphasizing urgent needs such as:
  - a. Standards for **smart contracts** under the Data Act;
  - b. Support for **Digital Euro and MiCA** compliance;
  - c. Methods for assessing the **environmental impact** of DLTs;
  - d. Greater inclusion of **W3C DID/VC standards** for digital identity interoperability.
- **Community and Ecosystem Standards** Beyond formal SDOs (e.g., ISO, IEEE, ITU-T), the report recognizes the influence of **open-source and community-driven standards**, such as Ethereum's EIPs/ERCs and Hyperledger projects, which serve as de facto standards in many blockchain implementations.
- **Sector-Specific Use Cases and Gaps** Contributions from SEEBLOCKS-funded researchers and partners spotlight emerging needs in sectors such as:
  - a. **Healthcare** (secure data sharing and segmentation using blockchain);
  - b. **Automotive** (hybrid consensus for Internet of Vehicles);
  - c. **Carbon markets** (blockchain-enabled sustainability tracking);
  - d. **Intellectual property** (NFT standards and on-chain rights management).

- **Strategic Recommendations** The report provides actionable guidance to strengthen blockchain standardisation, including:
  - a. Incentivizing standard adoption through conformance testing and compliance tooling;
  - b. Developing ethics-by-design and trust frameworks to ensure transparency and fairness;
  - c. Advancing interoperability via modular IBC (inter-blockchain communication) architectures;
  - d. Embedding sustainability, accessibility, and security across all new standards.
- **SEEBLOCKS Contributions** The project addressed key gaps in the landscape through:
  - Research funding targeting EU priorities (Digital Euro, ESG, compliance);
  - Organizing standardisation workshops and community engagement events;
  - Supporting new EU-aligned standards proposals and pilot implementations.

## Conclusion

This final report reaffirms the critical role of coordinated standardisation in enabling blockchain and DLT adoption across Europe. By mapping the current landscape, identifying key deficiencies, and aligning with EU policy instruments, SEEBLOCKS offers a roadmap for fostering a robust, interoperable, and ethically grounded blockchain ecosystem. Its findings serve as a vital reference for policymakers, standards bodies, industry leaders, and academic researchers committed to advancing digital sovereignty and technological innovation in the EU.

# Table of Contents

<b>Executive Summary</b>	4
<b>Table of Contents</b>	7
<b>List of Tables</b>	8
<b>List of Figures</b>	8
<b>Abbreviations</b>	9
1. Introduction	10
<b>2. Landscape Analysis</b>	11
2.1 Blockchain Industry Community Standards	14
2.2 Major Blockchain Ecosystems	17
3. Gaps in Blockchain and DLT standardisation Landscape	19
3.1 Gap analysis based on Industry perspectives (1)	20
3.2. Gap Analysis based on EU Rolling plan for ICT Standardisation Priorities (2)	21
3.3. Further Identified Gaps - TWG and Literature-Based - (3)	22
4. SEEBLOCKS research and response to existing gaps	26
5. Conclusion	31
<b>6. References</b>	32
Annex 1	34
Summary of Blockchain & DLT Publications	36
Annex 2	40
List of all finalized ERC standards	40

## List of Tables

Table 1: An overview of standardisation groups.	11
Table 2: An overview of the hyperledger projects and their categorisation.	15
Table 3: Major Ethereum Standards.	15
Table 4: An overview of the notable open-source projects and standards by major ecosystems.	19
Table 5: Criteria Table of Concept and Standardisation.	19

## List of Figures

Figure 1. Distribution of standards across Priority Areas (SEEBLOCKS method)	13
Figure 2. Distribution of standards based on INATBA's taxonomy	14

## Abbreviations

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



Acronym	Description
<b>NB</b>	National (standards) body
<b>NC</b>	National committee
<b>NFT</b>	Non-fungible token
<b>NSB</b>	National Standard Bodies
<b>OID</b>	Object identifier
<b>PWI</b>	Proposed work item
<b>RFC</b>	Request for comment
<b>SDO</b>	Standard development organisation
<b>TC</b>	Technical committee
<b>TR</b>	Technical report
<b>TS</b>	Technical specification
<b>URI</b>	Universal resource identifier
<b>VASP</b>	Virtual asset service provider
<b>WD</b>	Working draft
<b>WG</b>	Working group
<b>WSC</b>	World Standards Cooperation
<b>ITU-T</b>	International Telecommunication Union - Telecommunication Standardization Sector
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>ANSI</b>	American National Standards Institute
<b>NIST</b>	National Institute of Standards and Technology
<b>UNE</b>	Una Norma Española (Spanish Association for Standardization)
<b>DIN</b>	Deutsches Institut für Normung
<b>ITSA</b>	International Token Standardization Association
<b>EEA</b>	Enterprise Ethereum Alliance

## 1. Introduction

Blockchain and Distributed Ledger Technologies (DLT) continue to play a transformative role in the modern digital economy and are regarded as a foundational technology in the European single digital marketplace. This report is the final report in a series of three Landscape Reports to be published by SEEBLOCKS.eu that provide an extensive analysis of the existing international standards landscape, identifying gaps, and presenting some concrete responses to address these, aiming to foster a cohesive and resilient blockchain ecosystem.

The first report, i.e., *D3.1 Blockchain & DLT Standards & Landscape Report*, described the context of international standards-making, elaborating the formal consensus processes that underpin the voluntary standards-making activities at international standards development organisations (SDOs) such as ISO, IEC and CEN contrasting these with the informal consensus-building that takes place at IEFT, W3C, and other open blockchain protocols such as Bitcoin, Ethereum, and other public blockchains.

The second report, i.e., *D3.3 Landscape and Gap Analysis Report on Blockchain/DLT Standardisation – Mid-Term Release*, provides an updated overview of the international standardisation landscape, expanding on previously identified gaps. It reviews recent publications, classifies new standards, and highlights contributions from formal bodies (e.g., ISO, ITU-T, IEEE) and community efforts (e.g., Hyperledger, ETHGlobal). The report further analyses existing gaps in areas such as consensus, interoperability, and permission, drawing on both industry perspectives and public consultation. It also outlines SEEBLOCKS' targeted responses to these gaps, including sponsored research, workshops, and use case development to support future standardisation priorities and promote EU digital resilience.

This report focuses on the current state of the art in blockchain standardisation, reviewing recent publications on emerging requirements and identifying common perspectives, gaps, and priority areas for future blockchain and DLT standardisation—ensuring that ongoing efforts remain aligned with market and societal needs. It expands the blockchain and DLT landscape and gap analysis by adopting three strategic perspectives: industry insights; findings from the SEEBLOCKS public consultation and the EU Rolling Plan for ICT Standardisation; and contributions from the SEEBLOCKS' Technical Working Group (TWG)<sup>1</sup>, alongside a review of the literature. In doing so, the report aligns with SEEBLOCKS.eu's mission to offer strategic analysis of the blockchain standardisation landscape and provide actionable recommendations to strengthen standardisation efforts. It also addresses key areas such as the current adoption and use cases of blockchain technology, recent technological developments, standardisation progress, remaining gaps, and future directions for research and development. As the final analysis of the project, this report serves as a critical checkpoint for SEEBLOCKS.eu, ensuring that its work is focused, informed, and effective in supporting the growth and resilience of the European single digital marketplace.

<sup>1</sup> <https://seeblocks.eu>

## 2. Landscape Analysis

This report builds on the first SEEBLOCKS report (D3.1) on the landscape analysis and the second report (D3.3-MT) on the landscape and gap analysis, providing an overview of Blockchain/DLT with a particular focus on the latest developments and publications in this area. D3.1 key areas were: 1) Blockchain in Europe and the importance of standardisation in this context, 2) Main standardisation bodies and industry representative bodies and the collaborative process behind creating open standards for blockchain and DLT, and 3) A number of key Blockchain and DLT standards published. This report expands on the second and third items by adding key analysis to the identification of standardisation gaps, particularly in areas highlighted through the SEEBLOCKS' TWG. It also raises discussion on what might be prioritised in the near future.

D3.1. provided a classification of the standardisation organisations and their consensus-making characteristics. There are a number of types of SDOs including international, regional, national and industry organisations that are all recognised as standards-making bodies. Industry standards, organisations, and consortiums are important in driving progress in blockchain and DLT standardisation. An overview of standardisation organisations, working groups, their focus areas in blockchain and DLT standardisation, and the number of their publications is presented in Table 1 below.

SDO	Organisation type	Committee/ Group	Focus Area	Standards Published
ISO	International	ISO/TC 307	DLT Standardisation	21
ITU-T	International	TSAG	DLT, ICT	35
IEEE	International	CTS/BSC, C/BDL, BOG/CAG, CTS/DFESC, IES/IES, PE/SBLC, C/SAB, EMB/StdCom	Blockchain, DLT, Consumer Technology, Digital Finance, Industrial Electronics, Smart Buildings, Standards Activities	19
ETSI	European	ISG PDL, IPv6 groups	Permissioned Distributed Ledger, IPv6	18
ANSI	National	ASC X9, X9A	DLT Terminology, Blockchain Risk Assessment	3
NIST	National	CSD, ACD	Blockchain Security, Cybersecurity	6
UNE	National	SC 307	Blockchain and Distributed Ledger Technologies	1
DIN	National	NA 043-0204 AA, NA 009-00-15-02 AK	DLT Specifications, Records Management	6
EEA	Industry	6 Active Working Groups	Enterprise Ethereum, Blockchain Leaders, Adopters, Innovators, Developers,	7

SDO	Organisation type	Committee/ Group	Focus Area	Standards Published
			Businesses	

*Table 1: An overview of standardisation groups.*

In the European context, there is a recognised and ongoing need for continuous monitoring of ICT standards. This need is underscored by Action 1 of the [EU Rolling Plan for ICT Standardisation](#), which calls for a sustained analysis of standardisation gaps and identification of appropriate solutions. In the area of blockchain and distributed ledger technologies (DLT), earlier literature has typically either focused on narrow domains—such as blockchain security standardisation [3], non-fungible tokens [2], or interoperability—or has offered high-level and outdated overviews, as seen in [4] and [5]. More comprehensive analyses were provided by ITU-T in 2019 [6] and ETSI in 2020 [7]; however, the ETSI report is limited to permissioned DLT systems, and both reports are now outdated.

Recent and more systematic efforts have significantly enhanced the understanding of the DLT standardisation landscape. The SEEBLOCKS project's D3.1 report (2023) and the INATBA systematisation of knowledge report (February 2024) together established a new baseline, identifying 95 relevant standard publications. These are listed in a live GitHub repository maintained by INATBA's DLT Standards and Working Group [9]. BLOCKSTAND has mirrored this list in its [Repository](#) of Blockchain Standards. Building on this foundation, the SEEBLOCKS D3.3 report (published in June 2024) introduced additional analysis and incorporated [ISO/TR 6277:2024—Blockchain and distributed ledger technologies — Data flow models for blockchain and DLT use cases](#) that was published in February 2024 and led by SEEBLOCKS Strategic Lead Fiona Delaney, consolidates system-level models from ISO 23257:2022 and ISO/TR 3242:2022. It presented a data-flow-centric description framework for DLT use cases, enhancing system design, governance, risk management, and interoperability, especially for hybrid or orchestrated environments.

This report builds upon all prior work—D3.1 (2023), INATBA (2024), and D3.3 (June 2024)—and further expands the catalogue of standards. As of this report, 116 standard publications are identified, representing an increase of 20 standards over the previous count. These standards, published by international, regional, and national standards development organisations, are detailed in Annex 1. This expanded and updated listing is the most comprehensive to date and will be integrated into the SEEBLOCKS Standards Visualisation Tool in due course.

In line with the analysis in the first Landscape Report (D3.1) and to achieve SEEBLOCKS objectives, the following set of **Priority Areas (PA)** for Blockchain and DLT have been selected along with **foundational** standards (See Annex 1 for more information). 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 on these niches or other relevant domains.

Figure 1 presents the distribution of standards across the PAs in 2025, as determined by SEEBLOCKS.

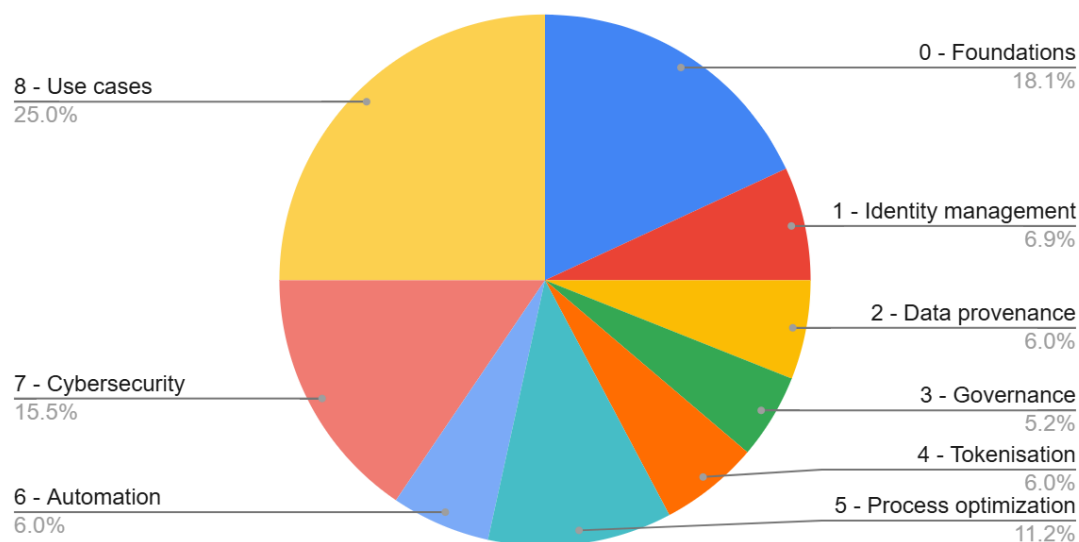


Figure 1. Distribution of standards across Priority Areas (SEEBLOCKS method)

In addition, the taxonomy proposed by INATBA classifies these standards according to Level 1–3 criteria, based on ISO/TS 23258:2021. The Level 1 concepts include: Asset, Consensus, Smart Contract, Entity, Governance, Interoperability, Ledger, Permission, Record, Security, Service, System, Technology, and Trust. Each Level 1 concept is further refined into Level 2 categories—for example, *Asset* is broken down into *Digital Asset* and *Provenance*. These in turn are subdivided into Level 3 concepts, such as *Digital Asset – Cryptographic Asset* and *Provenance – Origin of Asset*, *History of Asset*, *History of Custody*, and so forth for each Level 1 concept. Figure 2 illustrates the distribution of 116 standards based on the taxonomy proposed by INATBA (See Annex 1 for more information).

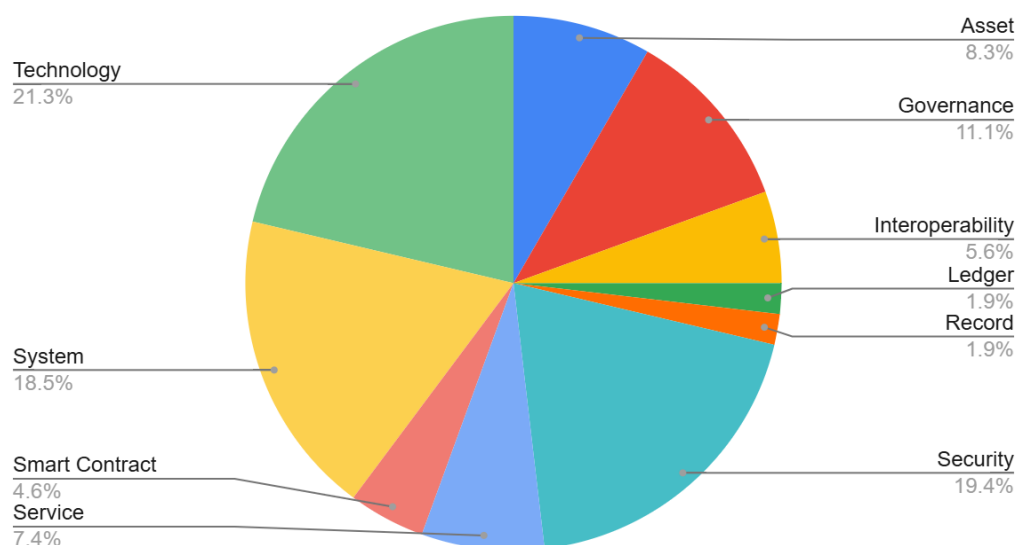


Figure 2. Distribution of standards based on INATBA's taxonomy

## 2.1 Blockchain Industry Community Standards

While the INATBA report places protocol and smart contract standards (interface and application-specific, open blockchain protocols e.g. Ethereum Enterprise Alliance) outside their scope, SEEBLOCKS research prefers to include these important open-source community efforts (usually occurring through informal RFC processes). D3.1 presented such standards, with a specific focus on the Ethereum Improvement Proposals (EIP) and Ethereum Request for Comments (ERC) and the early SEEBLOCKS public consultation report evidences the importance of these community standards, and in the case of the respondents to the public consultation many had taken an active role in the development of such standards. Hence, a full landscape analysis on Blockchain and DLT standardisation would not be complete without reference to these industry community or protocol standards. DLT standards development has been most actively done by industry and community organisations. Their work is different from that of formal standards-developing organisations, as the specifications developed are usually published with an accompanying repository of open-source implementation code.

The Linux Foundation is an example of a community-driven organisation that provides support for a range of cross-industry blockchain applications. Hyperledger, hosted by the Linux Foundation, presently has a community of over 200 companies that are focused on the development and implementation of enterprise blockchain. Notably, their work has led one of their frameworks, Hyperledger Fabric, to be considered as a de facto standard for enterprise blockchain platforms. An overview of the Hyperledger projects and their categorisation is presented in Table 2.

Hyperledger Project	Category
Solang	Tools
Iroha	General-Purpose Distributed Ledger
Indy	Decentralized Identity
Firefly	Connectivity/Integration Gateway
Fabric	General-Purpose Distributed Ledger
Cello	Deployment Automation
Caliper	Performance Benchmarking
Cacti	Cross-Chain Interoperability
Bevel	Deployment Automation
Besu	General-Purpose Distributed Ledger
Aries	Decentralized Identity
Anoncreds	Decentralized Identity
Web3j	Ethereum Integration Library
Identus	Decentralized Identity

Table 2: An overview of the hyperledger projects and their categorisation.

Ethereum's evolution is guided by the EIP process, an open, [GitHub-based](#) workflow where anyone can propose protocol upgrades, optimizations, or application-layer conventions. Each EIP follows a structured path—drafting, community review, core-dev discussion, and eventual acceptance or rejection—ensuring that both consensus changes (e.g., consensus-layer upgrades) and interface standards benefit from broad community input.

Beyond the meta-governance of EIPs, the Ethereum community has introduced a suite of ERCs that define widely adopted token interfaces, proxy patterns, signature schemes, and even human-readable naming. These standards, together with open-source reference libraries and developer tools, form the backbone of Ethereum's interoperable ecosystem. The main standards of Ethereum are listed in Table 3 and a complete list of finalized ERC standards are provided in Annex 2.

Standard	Category	Purpose / Description
EIP-20 (ERC-20)	Fungible Token Interface	Defines a common API for fungible tokens (totalSupply, balanceOf, transfer, approve, transferFrom).
EIP-721 (ERC-721)	Non-Fungible Token (NFT)	Standardizes unique, indivisible tokens with metadata and ownership methods for collectibles.

Standard	Category	Purpose / Description
Interface		
EIP-1155	Multi-Token Interface	Enables a single contract to manage fungible, non-fungible, and semi-fungible tokens together.
EIP-777	Advanced Fungible Token	Backward-compatible ERC-20 alternative with hooks for send/receive and operator management.
EIP-4626	Tokenized Vault Standard	Defines a common API for yield-bearing vaults, facilitating cross-protocol integrations.
EIP-2612	Permit (ERC-20 Upgrade)	Adds permit() to ERC-20 to approve token transfers via off-chain signatures (gasless approvals).
EIP-165	Interface Detection	Standard method (supportsInterface) for contracts to declare which interfaces they implement.
EIP-1820	Universal Interface Registry	On-chain registry mapping addresses to the interfaces they implement, enabling dynamic introspection.
EIP-1967	Proxy Storage Slots	Specifies fixed storage slots for proxy patterns, standardizing how implementations locate logic.
EIP-2535 (Diamonds)	Modular Proxy ("Diamond") Standard	Enables a single proxy to be composed of multiple modules ("facets"), each handling different functionality.
EIP-712	Typed Structured Data Signing	Defines domain-separated, typed data hashing for secure and human-readable off-chain signatures.
EIP-1271	Contract-Based Signature Validation	Standard for verifying signatures issued by smart contracts (useful for multisig and wallets).
EIP-137 (ENS)	Ethereum Name Service	Specifies a decentralized naming system, mapping human-readable names (e.g., alice.eth) to addresses.
EIP-4337	Account Abstraction via EntryPoint	Introduces a "UserOperation" standard to decouple accounts from EOAs, paving the way for smart-contract wallets and paymasters.
EIP-725 / EIP-735	Identity & Claims	Defines proxy-based identity wallets (EIP-725) and a claims registry (EIP-735) for decentralized identity.

Table 3: Major Ethereum Standards.

Community standards extend well beyond Hyperledger and Ethereum. In the wider blockchain ecosystem, active communities drive:

- Open-source reference implementations, ensuring that any developer can inspect, reproduce and extend protocol code;
- Transparent improvement processes, modelled on RFC-style or on-chain governance frameworks, which solicit and vet proposed changes publicly;
- Reusable tooling, from language-agnostic SDKs and testing suites to interoperability bridges and security-audit frameworks, is designed to promote cross-chain compatibility, resilience, and rapid innovation.



In the following section, the results of the analysis of some of the major ecosystems is presented.

## 2.2 Major Blockchain Ecosystems

The following ecosystems represent some of the most technically advanced, widely adopted, and community-driven blockchain platforms in the current landscape. Each of them demonstrates significant activity in open governance, standardisation processes, and open-source tooling, all of which are essential for evaluating the maturity and interoperability of blockchain infrastructures. They also span a diverse range of consensus mechanisms, smart contract languages, identity frameworks, and application domains (e.g., DeFi, NFTs, SSI, and enterprise blockchain), providing a representative cross-section of the broader blockchain ecosystem. This selection ensures that the analysis captures both public blockchains with high developer engagement (e.g., Ethereum alternatives like Solana, Avalanche, Algorand) and permissioned or enterprise-aligned efforts (e.g., IBM/ToIP). Each ecosystem contributes uniquely to the evolving standards landscape and collectively illustrates the breadth of innovation and governance models in the space.

The Algorand Foundation manages an open RFC-style process (Algorand Requests for Comments, or ARCs) for evolving protocol features (e.g. ARC-20 token interfaces, ARC-69 metadata conventions). All core implementations—from the Go node to SDKs in JavaScript, Python, and higher-level smart-contract frameworks like PyTeal—are open-source. Recent additions like AlgoKit, an end-to-end dApp development toolkit, exemplify Algorand's commitment to community-maintained tooling.

Solana Program Library (SPL) provides canonical on-chain programs (notably the SPL Token program) for fungible and non-fungible assets, ensuring cross-app interoperability. The community-developed Anchor framework further simplifies smart-contract development with Rust macros, client code generation, and built-in security checks. Together, SPL and Anchor form the de facto standards for Solana dApps.

Cardano Improvement Proposals (CIPs) govern everything from native token formats to wallet interoperability, managed on public Git repositories. Its core tooling—Plutus (Haskell smart-contract platform) and Marlowe (financial DSL)—is fully open-source. The Atala PRISM identity toolkit implements W3C DID/Verifiable Credential standards on Cardano, reflecting a community-led approach to self-sovereign identity.

Bitcoin's decentralized governance relies on Bitcoin Improvement Proposals (BIPs) and multiple client implementations (Bitcoin Core, Bitcoin Knots). Layer-2 innovation such as the Lightning Network uses open BOLT specifications to ensure cross-implementation compatibility. Identity extensions like ION (a Sidetree-based DID overlay) further demonstrate community-driven standards on top of Bitcoin.

The TRON ecosystem employs TRON Improvement Proposals (TIPs) for protocol upgrades and token specs (TRC-20/TRC-721). By open-sourcing BTFS (BitTorrent File System), TRON integrates decentralized storage via an IPFS-derived standard. Community-maintained SDKs such as TronWeb and API gateways like TronGrid round out its open-source stack.

TON (The Open Network) was relaunched by the Telegram community via fully open governance and a nonprofit foundation. Its core node software, sharding design, on-chain services (TON DNS, TON Storage), and emerging Society DAO governance model are all developed through public contests, Git repositories, and forum-based proposals.

Stellar's development is guided by Core Advancement Proposals (CAPs) for protocol changes and Stellar Ecosystem Proposals (SEPs) for application-layer standards (e.g. SEP-6/SEP-24 for fiat on/off-ramps, SEP-10 for web-auth). The open-source Stellar Core and Horizon server, together with community-run anchor implementations, power its interoperable payment network.

Avalanche Improvement Proposals (AIPs) enable on-chain governance by AVAX holders. Community frameworks like Subnet-EVM and HyperSDK let anyone spin up EVM-compatible subnets, while Avalanche.js provides a comprehensive JavaScript API. Open bridges and grant-backed ecosystem tools exemplify its modular, community-first design.

Beyond public chains, IBM has co-founded the Trust over IP (ToIP) Foundation for cross-platform identity standards (W3C DIDs/VCs), contributed to the Token Taxonomy Framework for technology-agnostic token definitions, and open-sourced the Blockchain Automation Framework (BAF) for cloud deployment of enterprise ledgers.

Tezos pioneered self-amendment via on-chain voting by XTZ holders. Off-chain, Tezos Improvement Proposals (TZIPs) define token interfaces (FA1.2, FA2 multi-asset standards) and metadata formats (TZIP-16). Community languages (SmartPy, LIGO) and the Taquito JS SDK further standardize contract development and integration.

Under the Antelope Coalition, EOS and sister chains collectively maintain the open-source Antelope framework (formerly EOSIO). Community-driven working groups produce Inter-Blockchain Communication (IBC) protocols and SDKs like WharfKit, while token-holder governance allocates funding to ecosystem improvements. An overview of the notable open-source projects and standards by major blockchain ecosystems is presented in Table 4.

Ecosystem	Community-Driven Standards & Tooling
Algorand	ARCs (e.g. ARC-20, ARC-69), Algorand Node (Go), PyTeal, AlgoKit
Solana	SPL (Token, NFT programs), Anchor framework, Solana Name Service
Cardano	CIPs (e.g. CIP-20 token, CIP-31 metadata), Plutus, Marlowe, Atala PRISM
Bitcoin	BIPs (SegWit, Taproot), Lightning BOLT specs, ION DID overlay
TRON	TIPs (TRC-20, TRC-721), BTFS, TronWeb, TronGrid
TON	Open-source node & sharding, TON DNS, TON Storage, Society DAO governance
Stellar	CAPs, SEPs (6, 10, 24), Stellar Core, Horizon, Anchor implementations
Avalanche	AIPs (on-chain governance), Subnet-EVM, HyperSDK, Avalanche.js, Avalanche Bridge
IBM Blockchain Platform	Trust over IP (DID/VC stack), Token Taxonomy Framework, Blockchain Automation Framework
Tezos	On-chain amendment, TZIPs (FA2, metadata), SmartPy, LIGO, Taquito
EOS/Antelope	Antelope core framework, Antelope IBC, WharfKit SDK

Table 4: An overview of the notable open-source projects and standards by major ecosystems.

### 3. Gaps in Blockchain and DLT standardisation Landscape

This section identifies the current gaps that need to be addressed within Blockchain and DLT standardisation. We approach the topic from three strategic points of views: 1) Industry informed, 2) The SEEBLOCKS Public Consultation findings and the EU Rolling plan for ICT standardisation (2025), and 3) The SEEBLOCKS' TWG contributions and the review of the literature.

As aforementioned, the first analysis on the existing gaps employs an industry perspective informed by research outputs from INATBA and SEEBLOCKS.eu. INATBA has presented an analysis of how well different areas (as described by Level 1 criteria/concepts) are represented regarding the number of standards, followed by an examination based on several factors. The determination of whether a concept should receive further standardisation can be made by considering the following criteria. INATBA defined criteria A, B, C, and SEEBLOCKS added criteria D and E.

ID	Description	Example
Note A-C are defined by INATBA, while D and E are SEEBLOCKS.eu additions.		
A	Concept is not DLT specific and can therefore be (or already is) covered by a standard that is not DLT specific.	eg. Reference Architecture (ISO 23257:2022, ITU-T F.751.2)

ID	Description	Example
B	Concept is partially covered by a DLT standards publication which is categorised in a different (e.g. higher level) category, thus the need for a dedicated standard does not exist.	eg. Guidelines for governance (ISO 23635:2022)
C	Concept would benefit at least one main stakeholder group (users, regulators, infrastructure providers, node operators)	eg. Decentralised Media Rights Application Format (ISO/IEC 23000-23)
D	Concept is rapidly evolving, necessitating frequent updates to maintain relevance.	eg. Security requirements for digital integrity proofing service based on DLT (ITU_T X.1407)
E	Concept intersects with other emerging technologies, requiring a multidisciplinary standardisation approach.	eg. OID-based resolution framework for transaction of distributed ledger assigned to IoT resources (ITU_T Y.4476)

Table 5: Criteria Table of Concept and Standardisation.

### 3.1 Gap analysis based on Industry perspectives (1)

Figure 1 shows that some areas have more dedicated standards than others, with the best-represented ones focused on foundational or system-level concepts. However, identifying a gap on the basis of the number of related standards is simplistic. Hence, we need the criteria A-E defined here for further analysis. Following this analysis, we will further focus on 3 areas: Consensus, interoperability, and Permission.

#### Consensus

While it is a requirement for any distributed system, there are few publications specifically addressing consensus for DLTs. It is our view that ISO TS 23635:2022 Guidelines for Governance (per Criteria B) take a high-level view of consensus, but that deeper exploration can be useful. Apart from the Nakamoto Consensus, the sub-concepts of Consensus are still generic to distributed systems. Considering that consensus is integral to a DLT's integrity, functionality, and performance, dedicated standards for consensus in DLTs are key. Moreover, as consensus mechanisms are rapidly evolving (criteria D), with new approaches being proposed frequently, standardisation efforts in this area would require regular updates to stay relevant.

#### Interoperability

Despite there being five publications on interoperability, their applicability is somewhat limited due to their narrow focus and scope. Specifically, three of these are produced by the European Union Agency for

Cybersecurity (ENISA) and the European Blockchain Services Infrastructure (EBSI), making them primarily relevant to Ethereum-based infrastructures and not easily generalisable to other DLT ecosystems. Another publication concentrates on interoperability between DLTs and the Internet of Things (IoT), which, while valuable, does not address broader cross-platform DLT interoperability. This highlights a clear gap in the availability of a high-level, technology-agnostic interoperability standard that can be applied across various DLTs and use cases.

Moreover, given that DLT interoperability often intersects with other emerging technologies such as IoT, 5G, and AI (criteria E), a multidisciplinary approach to standardisation would be more appropriate. Much emphasis is currently placed on ISO/CD TS 23516 Blockchain and DLT Interoperability Framework, which aims to address this broader need, but it remains in the early Committee Draft stage, indicating that a mature, universally applicable standard is still under development.

### Permission

A key concept in maintaining IT system security is permissioned access. DLTs present unique challenges due to the large number of different actors trying to access the system and communicate to reach a consensus. Permission and its sub-concepts would greatly benefit from dedicated DLT standardisation, as opposed to just general standards. The absence of DLT publications in this category underscores that standardisation of the sub-concepts of Permission should be a priority. This is particularly important as we anticipate an increasing number of permissioned DLT systems to be deployed by enterprises, consortia, and governmental bodies for various use cases in the future. The rapid evolution of these systems (criteria D) further emphasises the need for adaptable standardisation in this area.

These three areas are also pointed out by INATBA as in need of further standardisation efforts. Moreover, INATBA's is pointing out the following concepts in need of further standardisation efforts: Governance (with 1 publication only), Smart Contracts, Asset (with focus on the Provenance), Record and Service.

### 3.2. Gap Analysis based on EU Rolling plan for ICT Standardisation Priorities (2)

The second analysis focuses on actions outlined by the EU Rolling Plan for ICT Standardisation (24<sup>2</sup> and 25 editions<sup>3</sup>). These actions were formulated based on missing elements in the current Blockchain and DLT standardisation landscape. Moreover, we also took into account the results of SEEBLOCKS public consultation. The analysis concluded with the following recommendations and areas in need of attention from the standardisation community:

- Standardisation of the operation and reference implementation of permissioned distributed ledgers and distributed applications, with the purpose of creating an open ecosystem of industrial

<sup>2</sup> <https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2024>

<sup>3</sup> <https://interoperable-europe.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2025>

interoperable solutions” (Action 4 of the Rolling Plan). The need for standards addressing the Permission concept was also highlighted in the previous analysis;

- Develop standards aligned with the Data Act legislative proposal, particularly concerning the essential requirements for smart contracts. This recommendation is outlined in Action 6 of the Rolling Plan. Additionally, the SEEBLOCKS public consultation highlights the significance of the Data Act within the blockchain and DLT standardisation landscape. According to the consultation, 20% of respondents identified the Data Act as the most important EU legislation, regulation, or policy in this context. It ranked third, following the Markets in Crypto-Assets Regulation (2019), cited by 25% of respondents, and the Framework for EU Digital Identity (2021), cited by 22.5%;
- Develop the standards needed for the introduction of Digital Euro (CBDC), and for digital assets (MiCA Regulation), in particular to ensure interoperability with smart-contracts, legacy systems, etc, linked with either CBDCs or private money - Action 7 of the Rolling Plan. The importance of Digital Euro is also highlighted through the SEEBLOCKS public consultation. This was ranked in fourth place overall in terms of its importance in the Blockchain and DLT standardisation landscape, with 17.5% of the respondents considering Digital Euro as the most important in this context;
- Develop standards towards assessing CO2 footprint of different blockchains/DLTs, MiCA, EU Sustainable Finance taxonomy. This gap is highlighted through Action 8 of the Rolling Plan. In addition, SEEBLOCKS public consultation also identifies the importance of addressing sustainability matters;
- Continuous investigation of new potential use cases for Blockchain and DLT and analysis on the need for their standardisation (Action 1 and Action 3 of the Rolling plan).

### 3.3. Further Identified Gaps - TWG and Literature-Based - (3)

While the above captures the core Rolling Plan actions and public-consultation feedback, the following extensive set of missing elements emerged from the detailed SEEBLOCKS landscape and gap analysis, as well as expert comments gathered through the SEEBLOCKS' TWG:

#### 1. Motivation for Blockchains to Adhere to Standards

- **Economic and Operational Incentives:** Beyond technical interoperability, demonstrable case studies should be established. For example, pilot projects measuring time-to-market reduction and integration cost savings when adopting common consensus-layer APIs, data schemas (e.g., JSON-LD, CBOR), and messaging formats. Such benchmarking reports will help projects build a clear business case for early standards adoption under Action 4;
- **Shared Security Assurance:** Creation of joint vulnerability-disclosure and patching protocols across platforms. A formal ISO/IEEE-aligned standard for security testing and certification (e.g., conformance to TC 307 security guidelines, penetration-testing

baselines, key-management profiles) will incentivise networks to align their security and key-rotation processes;

- ***Institutional Adoption Drivers***: Produce standardised “compliance scorecards” for ISO/TC 307, IEEE P2418.x and sectoral frameworks (finance, supply chain, agriculture). Publishing machine-readable compliance manifests (supported specs, tested versions, deviations) reduces auditing overhead for regulators and enterprises.

## 2. Regulations as Motivation vs. Deterrent

### Positive Motivators:

- ***MiCA Harmonisation***: Formal standards for stablecoin reserve attestations and smart-contract audit requirements will ease institutional issuers’ regulatory compliance (Action 7);
- ***Data Act Requirements***: Specify normative clauses for smart-contract source-code transparency, standard event-logging formats, and data-sharing interfaces (RESTful/GraphQL APIs) to fulfil Data Act obligations under Action 6;
- ***GDPR-Driven Privacy Standards***: Define permissioned-network access-control models (RBAC, ABAC) and zero-knowledge proof patterns for on-chain pseudonymity, supporting Action 4 implementations.

### Deterrents to Avoid:

- ***Overly Broad Token Classification***: Advocating for technology-neutral asset definitions distinguishing utility vs. security tokens in MiCA to prevent blanket security-law treatment that stifles DeFi innovation;
- ***Fragmented KYC/AML Mandates***: Harmonise FATF-style “travel rule” implementations via a unified data schema (e.g., ISO 20022-compatible message packets) to reduce cross-border compliance costs;
- ***One-size-fits-all Licensing***: Encourage proportionate licensing tiers for low-value CBDC and micropayment transactions to foster Digital Euro usage rather than deter small-value transactions.

## 3. W3C Standards – Decentralized Identity & Credentials

- ***DID & VC Profiling***: Profile W3C DID Core 1.0 and VC Data Model v2.0 for EU use cases—e.g., CBDC KYC/AML flows, eIDAS 2 ‘wallet’ interoperability, and EBSI anchor integration (Action 10);
- ***Leverage Blockchain2 CG Outputs***: Incorporate high-level application-architecture requirements from the W3C Blockchain2 Community Group into Rolling Plan Actions 1/3, ensuring web-native DLT apps leverage standard DID/VC stacks;



- **Interoperability with eIDAS:** Map DID Authentication Workflows to eIDAS 2 Credential Service Provider (CSP) profiles, avoiding parallel European identity specs that replicate global W3C work.

#### 4. Ethics and Compliance Standards

- **Ethics-by-Design Framework:** Establish an IEEE P7000-style standard for blockchain, mandating embedded fairness controls, informed-consent protocols, and transparent algorithmic-decision reporting within smart-contract templates;
- **ESG & Sustainability Certification:** Extend Action 8 by defining machine-readable carbon-accounting formats for on-chain CO<sub>2</sub>-monitoring, aligned with EU Sustainable Finance taxonomy JSON Schema and MiCA disclosure rules;
- **Global Compliance Reference Architectures:** Publish open-source reference architectures for multi-jurisdictional AML/KYC/data-localization compliance modules (plug-and-play smart-contract libraries).

#### 5. Building Public Trust

- **DLT Trust Framework Standard:** Develop a cross-SDO standard (ISO, IEEE, CEN/CENELEC) for trust metrics—transparency score, auditability index, dispute-resolution SLA—that can be embedded into DLT platforms and DAOs;
- **Conformance & Certification Schemes:** Launch EU-recognized trust-certification (similar to ISO IEC 27001) specifically for blockchain networks, covering ethical, operational, and technical compliance;
- **Human-Centric UX/UI Guidelines:** Create standardized wallet-and-dApp interface guidelines: human-readable risk warnings, standardized consent flows, accessibility requirements for low-literacy users. Publish these as part of Action 4 toolkits;
- **Decentralized Insurance & Compensation Protocols:** Define and standardise on-chain insurance frameworks—such as mutual-insurance pools, protocol reserve funds, and reversible-transaction escrow standards—to guarantee user recourse for hacks, smart-contract exploits, or accidental transfers. Integrate transparent insurance disclosures and metadata into certification schemes, and display “insurance-backed” trust marks within wallet and dApp interfaces to signal coverage status;
- **Wallet Trust & Safety Standards:** Establish comprehensive wallet-design specifications mandating features like address-checksum validation, human-readable naming resolution (e.g., ENS/FIO), integrated phishing and blacklist warnings, transaction simulation previews, and optional reversible-transfer escrow mechanisms. Develop conformance test suites for wallets to validate compliance with these trust and security guidelines, and create a “wallet trust badge” program to certify compliant software.

#### 6. Inter-Blockchain Communication (IBC)



- **Vendor-Neutral Reference Architecture:** Built upon ISO/TS 23516 to define layered IBC components—transport, authentication, relay coordination, state verification—with mappings to IETF/W3C networking specs;
- **Standardised Cross-Chain Message Formats:** Define universal message schemas (fungible token ICS-20, metadata, consensus proofs, permissions headers, event logs) extensible to CBDC and private-money scenarios (Action 7);
- **Security Assurance Levels & Test Frameworks:** Introduce conformance-testing suites with security-level grades (penetration-testing profiles, formal-verification artifacts) for bridges and cross-chain relayers.

## 7. Intellectual Property (IP) Protection

- **Standardised NFT Metadata & Asset Identifiers:** Define open schemas (based on ISCC codes and standardized JSON-LD vocabularies) that distinguish proofs of authorship, ownership, licensing, and usage rights;
- **Legally Auditable Smart-Contract Templates:** Create certified rights-management contract templates (royalty splitting, revocation mechanisms, derivative permissions) that interoperate with centralised IP registries;
- **Cross-Chain IP Provenance Protocols:** Standardize on-chain/off-chain claim-resolution workflows, including dispute arbitration procedures, challenge windows, and on-chain evidence logs.

## 8. Decentralized Governance Protocols

- **Unified Governance Lifecycle Standard:** Specify metadata and interfaces for proposal submission, eligibility verification (on-chain KYC), quorum calculation, vote execution and emergency-override operations within DAOs;
- **Governance Conformance Testing:** Develop testbeds for governance resilience—stress-testing quorum thresholds, privacy of votes, anti-collusion analytics, and procedural fairness assessments;
- **Inter-DAO Voting & Cross-Chain Coordination:** Standardize governance-action message schemas to enable cross-DAO referenda and cross-chain multisig voting (supporting multi-chain ecosystems in Action 1).

## 9. Thematic & Sectoral Gaps

- **Supply Chain DLT Standards:** Harmonize GS1 Digital Link with blockchain data-hash schemas via middleware reference designs; publish interoperability guidelines for IoT-anchored DPP use cases;
- **DeFi Protocol Standardisation:** Create global DeFi technical standards for lending, AMM, synthetic-asset protocols, and on-chain oracles, endorsed by ISO TC 307 working groups;

- **Consensus-Mechanism Benchmarks:** Establish a common framework for comparing consensus algorithms (security assumptions, performance metrics, regulatory alignment), enabling informed protocol selection.

## 4. SEEBLOCKS research and response to existing gaps

Besides conducting a thorough analysis on Blockchain and DLT standardisation landscape and identifying existing gaps, SEEBLOCKS also aims to address some of these gaps. Specifically, we will focus on the work conducted by the SEEBLOCKS funded researchers through the SEP calls (see more details on SEP in the SEEBLOCKS deliverables focused on calls monitoring and impact: D2.1, 2.2, 2.3 and 2.4). Their work addresses several of the gaps identified, as it is detailed below. Other relevant project activities aiming at closing this gap are considered as well.

**Identified Gap/Recommendation - Develop the standards needed for the introduction of Digital Euro (CBDC), and for digital assets (MiCA Regulation), in particular to ensure interoperability with smart-contracts, legacy systems, etc, linked with either CBDCs or private money**

SEEBLOCKS' response to this gap:

- SEEBLOCKS Researcher Dymitar Kyosev's project, Digital Euro - Private Enforcement on Debt, is a specific response to this gap. The project aims to propose a standardisation approach for private payment service providers to adapt their internal procedures to the upcoming Digital Euro.

**Identified Gap/Recommendation - Develop standards towards assessing CO2 footprint of different blockchains/DTLs, MiCA, EU Sustainable Finance taxonomy/Sustainability topic**

SEEBLOCKS' response to this gap:

- SEEBLOCKS Researcher Belen Suarez' project is a specific response to this gap. Her funded project is conducting activities within the Working Group (WG) at CEN/Cenelec JTC19 WG2 Environmental Sustainability of Blockchain and Distributed Ledger Technologies. The WG aims to develop a set of European standards for the environmental (climate) sustainability of Blockchain and DLTs. Belen worked on the draft of the Technical Report on the environmental sustainability classification methodology of the Blockchain and DLTs consensus mechanisms (this was circulated for approval) and is currently continuing the preliminary research, administrative works and stakeholder engagement necessary to launch the ballot for approval of the Technical Specification that aims to provide a complementary classification of Environmental Sustainability Taxonomy of Blockchain and DLT which pursues to support as the basis for labelling these technologies and crypto assets according to energy efficiency categories;
- SEEBLOCKS Researcher Shakira Bedoya Sanchez's project is also tangential to this gap. Shakira is funded by SEEBLOCKS to actively engage in AHG3 FinTech in Carbon Markets under TC322 (Sustainable Finance) and is working concurrently on:

- Standardisation in Carbon calculation (effectiveness and accountability): Revision of ISO 14016:2020 (Environmental Management Guidelines on the assurance of environmental reports);
- Standardisation in Carbon Market Methodologies: Partake in the standardisation work of ISO/WD TS 23516 (Blockchain and Distributed Ledger Technology Interoperability Framework) and ISO14068 (Greenhouse gas management and climate change management and related activities, Carbon neutrality);
- Standardisation in quality assurance of ETS (Development of Technical Reports).
- SEEBLOCKS researcher Paul Ferris, aims as part of the SEEBLOCKS funded projects, drafted a new sustainability section for the ISO/TC307 Strategic Business Plan and hence developed new standards with a sustainability focus.

**Identified Gap/Recommendation: Continuous investigation of new potential use cases for Blockchain and DLT and analysis on the need for their standardisation**

One of SEEBLOCKS responses to this gap/recommendation was the organisation of a workshop (Blockchain Nexus: Bridging Innovations and Standards for Tomorrow's Digital Frontier)<sup>4</sup> in conjunction with IEEE COMPSAC that took in Japan, between 2nd and 4th of July 2024. This international workshop invited researchers from both academia and industry to present their contributions to the Blockchain and DLT standardisation field, with a specific focus on the identification of new Blockchain use cases and the analysis of the need for their standardisation. The workshop received various contributions, including some from SEEBLOCKS funded researchers. Four papers were accepted for publications and their contributions are addressing the aforementioned gaps and some more. More information on these papers is presented next.

***Dimitar Kyosev, Distributed Ledger Technology as a Tool for Voluntary Standardization Compliance in Emerging Technologies: A Legal View***

This paper makes the case for empowering the users to police the voluntary standards. Utilising Distributed Ledger Technology (DLT), more precisely Directed Acyclic Graph – which reduces the costs of recording and storing individual measurements for each product allowing users to claim compensation every time the product does not perform according to specifications. The paper discusses the specific requirements the product should meet to utilise DLT as a compliance tool. It is also discussing the specific legal issues that entail from empowering users to police standard compliance.

<sup>4</sup> <https://ieeecompsac.computer.org/2024/blockchain-nexus/>

*Ramin Ranjbarzadeh, Ayse Keles, Martin Crane, Shokofeh Anari and Malika Bendeckache.* **Secure and Decentralized Collaboration in Oncology: A Blockchain Approach to Tumor Segmentation**

This research presents a novel use case for Blockchain, an innovative framework that uses blockchain technology to improve tumour segmentation in medical imaging. The approach tackles issues related to data security, particularly when dealing with real private datasets, annotation accuracy, and collaboration. With the growing reliance of the medical industry on accurate tumour segmentation from medical images for cancer diagnosis and treatment, current methods are inadequate in maintaining data accuracy and promoting collaboration among experts across different countries. Our suggested approach utilises blockchain technology to establish a decentralised, secure platform for the collaborative obtaining, annotation, and validation of medical images by data scientists, oncologists, and radiologists. Smart contracts streamline essential procedures such as verification of annotations, consensus among experts, and remuneration of contributors, guaranteeing the dependability and excellence of the data. Furthermore, the unchangeable record of transactions in the blockchain ensures a reliable basis for implementing artificial intelligence and machine learning algorithms. This improves the accuracy of segmenting data and allows for predictive modelling. This strategy not only improves the precision and effectiveness of tumour segmentation but also promotes a worldwide collaborative environment, which has the potential to revolutionise cancer diagnostics and treatment planning. Furthermore, it ensures the privacy and security of patient data.

*Mohammad Fardad, Elham Mohammadzadeh Mianji, Gabriel-Miro Muntean and Irina Tal,* **Hybrid Consensus Networks for Scalable and Secure Internet of Vehicles**

Permissioned distributed ledgers (PDLs) provide security and trust for Internet of Vehicles (IoV) applications, but face scalability issues due to resource-intensive consensus mechanisms. To address this, we propose a novel hybrid consensus network (HCN) architecture that leverages the computational capabilities of parked connected autonomous vehicles (CAVs) through a multi-layer vehicular edge computing (VEC) framework. The HCN is designed following guidelines outlined by ETSI regarding the structuring of PDLs. It aims to improve the performance, reliability and scalability of PDL-based IoV networks while maintaining their security and trust guarantees.

*Ruochen Qi and Dong-Hyu Kim,* **Geopolitical Manoeuvring in Blockchain Standardization: Comparative Analysis of the EU and U.S. Approaches**

This study examines the standardisation of blockchain technology and its applications across the EU, U.S., and ISO. It reveals the continued dominance of the U.S. in this field, driven by its focus on technological intricacies and institutional support, notably from NIST. Conversely, the EU's approach begins with reliance on ISO standards, potentially resulting in fragmented standardisation and limited proprietary blockchain development. The introduction of EUROCC as a competitor to USD-pegged stablecoins illustrates the EU's strategy to challenge U.S. technological

dominance, facilitated by initiatives like MiCA. This geopolitical manoeuvring underscores the EU's aspiration to solidify its position in the global blockchain landscape by leveraging standardisation as a tool for competitiveness and technological influence.

Other SEEBLOCKS project activities responded to this gap as well such as: the collection of use cases in the context of ETH Dublin, ETH Sofia, SEEBLOCKS's workshop on standardisation conducted in the context of the IEEE ICBC conference and through the open call for use cases on the project's website. All these use cases are available for consultation on the SEEBLOCKS website<sup>5</sup>. These events contributed to engaging the community (beyond the standardisation community) in standardisation activities. This is a very important aspect that should be continued (namely the engagement of the community in standardisation activities) as emphasized in the first "European Blockchain Standardisation Day"<sup>6</sup> organized by the SEEBLOCKS and BLOCKSTAND projects. The "European Blockchain Standardisation Day" took place on 9th April 2025 during the ISO TC 307 Plenary Week and brought together stakeholders from policy, industry, academia, and standardisation bodies to discuss the achievements and future pathways for blockchain innovation and standardisation in Europe.

#### **Identified Gap/Recommendation – Lack of clear motivational drivers for blockchains to adhere to standards**

SEEBLOCKS response to this gap:

Engage projects early with ISO/TC 307, IEEE P2418.x and relevant industry consortia to influence specifications; mandate modular network architectures so consensus, execution and storage layers can each evolve with new standards; adopt open, extensible on-chain metadata schemas (e.g. JSON-LD, CBOR, ERC-725); build and publish automated conformance test suites and versioned upgrade paths; and base cross-chain bridges on established inter-ledger protocols (e.g. Cosmos IBC, ILP) rather than bespoke adapters.

#### **Identified Gap/Recommendation – Unclear benefits vs. deterrents of regulation on existing blockchains**

SEEBLOCKS' response to this gap:

Promote proactive engagement with regulators (e.g. EU MiCA, SEC, FCA) and integrate regulatory requirements into system design from inception (audit trails, compliance reporting, identity frameworks); advocate for technology-neutral, balanced rules through policy consultations and sandbox programs; maintain transparent public records of compliance status; and embed compliance-by-design features—KYC/AML modules, on-chain disclosures and privacy controls—to transform regulatory constraints into competitive advantages.

<sup>5</sup> <https://seeblocks.eu/use-cases-list>

<sup>6</sup> <https://seeblocks.eu/events/european-blockchain-standardisation-day-seeblocks-blockstand>

### **Identified Gap/Recommendation – Under-representation of W3C standards in current mappings**

SEEBLOCKS' response to this gap:

Explicitly adopt W3C's DID Core 1.0 and Verifiable Credentials Data Model v2.0 as baselines for EU digital identity initiatives; support experts to W3C DID, VC and Data Integrity working groups; embed DID resolvers and VC issuance/verification libraries into core platforms with built-in audit logs and privacy controls; pilot end-to-end DID/VC flows in MiCA innovation hubs and EBSI prototypes; architect configurable identity modules that support multiple DID methods; and contribute to emerging W3C Blockchain2 community efforts to shape future web+DLT standards.

### **Identified Gap/Recommendation – Insufficient focus on ethics and compliance in standardisation efforts**

SEEBLOCKS' response to this gap:

Establish interdisciplinary ethics working groups drawing from legal, technical and civil society expertise; extend identity and security standards to include privacy-by-design, consent protocols and data-ownership safeguards; develop multi-jurisdictional compliance reference architectures; integrate ESG metrics into standards for consensus mechanisms and supply-chain use cases; launch ethical certification schemes modeled on AI and cybersecurity; and engage with international regulators to converge on global blockchain compliance norms, testing pilots in innovation sandboxes.

### **Identified Gap/Recommendation – Lack of standardised frameworks to build public trust in blockchain systems**

SEEBLOCKS response to this gap:

Create a DLT Trust Framework Standard via ISO TC 307, IEEE and CEN/CENELEC in collaboration with INATBA and civil-society groups; define auditability and explainability standards for smart contracts (human-readable descriptions, verification protocols, dispute-resolution methods); introduce third-party trust certification schemes; embed ethical design principles into technical specs for identity, data processing and governance; establish UX/UI guidelines for accessibility and risk communication; and showcase high-trust public use cases (e.g. transparent government spending, traceable supply chains) to demonstrate real-world benefits.

### **Identified Gap/Recommendation – Fragmented Inter-Blockchain Communication (IBC) and cross-chain standards**

SEEBLOCKS response to this gap:

Develop a modular, protocol-agnostic IBC reference architecture aligned with ISO/TS 23516 and interoperable with IETF and W3C network standards; define standardized message formats and metadata schemas for cross-chain asset/data transfers (consensus proofs, provenance, permissions, event logs); establish security assurance levels and conformance testing frameworks; promote baseline adoption of

Cosmos IBC, Polkadot XCM and Chainlink CCIP while ensuring alignment with EU and international standards; and launch cross-sector pilot projects and open-source interop testbeds under the EU Rolling Plan for ICT Standardisation.

### **Identified Gap/Recommendation – Absence of common standards for intellectual property protection in DLT**

SEEBLOCKS' response to this gap:

Define standard metadata formats and identifiers (e.g. ISCC codes, NFT schemas, digital fingerprints) distinguishing creator, owner, licensee and user rights; create legally auditable smart-contract templates for decentralised licensing, royalties, time-bound access and revocation; establish cross-chain provenance and dispute-resolution protocols; coordinate with ISO TC 307, WIPO, IEEE and Creative Commons on a global DLT IP Protection Framework aligned with existing treaties; and support industry-focused pilots (digital art, AI content, academic publishing) to validate these standards in practice.

### **Identified Gap/Recommendation – Need for standardised guidelines and protocols for decentralised governance**

SEEBLOCKS' response to this gap:

Develop a unified governance framework covering proposal lifecycle, eligibility criteria, quorum/voting thresholds, emergency override and dispute-resolution processes; standardize metadata and interfaces for governance smart contracts to ensure cross-platform transparency; produce best-practice toolkits and templates for DAOs; implement conformance testing and certification for governance protocols; foster international collaboration among ISO, IEEE, OECD and EU authorities; and run sandbox programs for high-stakes applications (cross-chain DAOs, DeFi, public infrastructure) to refine standards before broad deployment.

## 5. Conclusion

This final landscape and gap analysis review provides an updated overview of well-known international blockchain and DLT standards, taking into account the latest related publications and developments. It builds on the foundations laid in D3.1 and D3.3-MT by expanding the analysis of standardisation gaps, particularly those identified through the public consultation and TWG feedback documented in D3.3-MT. The report recognises contributions to international standards development through both formal and informal processes, and includes consideration of community-driven standards.

This document provides two strategic perspectives on gaps that exist and recommends further standards work be carried out under the headings of Consensus, Interoperability and Permission and furthermore, asserts that new standards be aligned with priority areas flagged in the EU Standardisation Rolling Plan in particular those that explore convergence and multi-technology domains. The Report also offers a deeper consideration of the research areas that SEEBLOCKS.eu has funded and provides an analysis of how these topics fit across the recommended targets outlined in the EU Rolling Plan.

Given the high level of activity across the industry, it is timely to develop standards that support both business and technical interoperability, especially at this current stage in the maturation of blockchain and DLT-enabled infrastructures.





## 6. References

- [1] Fiona Delaney, D3.1 Blockchain & DLT standardisation landscape report (2023)<https://zenodo.org/records/10797789>
- [2] Ko, Kyungchan, Taeyeol Jeong, Jongsoo Woo, and James Won-Ki Hong. "Survey on blockchain-based non-fungible tokens: History, technologies, standards, and open challenges." *International Journal of Network Management* 34, no. 1 (2024): e2245.
- [3] Chen, Xiaofeng, Zunbo Wei, Xiangjuan Jia, Peiyu Zheng, Mengwei Han, and Xiaohu Yang. "Current status and prospects of blockchain security standardization." In *2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, pp. 24-29. IEEE, 2022.
- [4] König, L., Korobeinikova, Y., Tjoa, S. and Kieseberg, P., 2020. Comparing blockchain standards and recommendations. *Future Internet*, 12(12), p.222.
- [5] Lima, C., 2018. Developing open and interoperable dlt/blockchain standards [standards]. *Computer*, 51(11), pp.106-111.
- [6] ITU Telecommunication Standardization Sector. ITU-T FG DLT D1.3 DLT standardization landscape. Technical report, ITU Telecommunication Standardization Sector, Geneva, CH, 2019. <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d13.pdf>.
- [7] European Telecommunications Standards Institute. ETSI GR PDL 001 V1.1.1 (2020-03) - Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies. Group report, European Telecommunications Standards Institute, Sophia Antipolis, FR, 2020.[https://www.etsi.org/deliver/etsi\\_gr/PDL/001\\_099/001/01.01.01\\_60/gr\\_PDL001v010101p.pdf](https://www.etsi.org/deliver/etsi_gr/PDL/001_099/001/01.01.01_60/gr_PDL001v010101p.pdf).
- [8] Kjell-Erik Marstein, Luke Riley and Ismael Arribas (2024). Systematisation of Knowledge: Distributed Ledger Technology Standardisation. International Association for Trusted Blockchain Applications (INATBA), Brussels, Belgium. [DLT Standardisation: A Comprehensive Report on Current Efforts and Future Directions - INATBA](#)

- [9] International Association for Trusted Blockchain Applications (INATBA). DLT Standards and Working Groups. GitHub repository. Retrieved 13 September 2023 from <https://github.com/quantnetwork/sok-dlt-standardisation>.
- [10] X. Jia, J. Xu, M. Han, Q. Zhang, L. Zhang, and X. Chen, 'International Standardization of Blockchain and Distributed Ledger Technology: Overlaps, Gaps and Challenges', *Computer Modeling in Engineering \& Sciences*, vol. 137, no. 2, 2023, doi: [10.32604/cmes.2023.026357](https://doi.org/10.32604/cmes.2023.026357).
- [11] Beck, R., Müller-Bloch, C., & King, J. L. (2018). Governance in the blockchain economy: A framework and research agenda. *Journal of the association for information systems*, 19(10), 1.
- [12] Lavayssière, Xavier, Tokenization of Financial Assets (2023). Available at SSRN: <https://ssrn.com/abstract=4649162> or <http://dx.doi.org/10.2139/ssrn.4649162>
- [13] Quant Network. (2024). *Blockchain in 2024: The year of institutional adoption*. Retrieved from <https://quant.network/perspectives/blockchain-in-2024-the-year-of-institutional-adoption/>
- [14] The Digital Chamber. (2025, March 25). *Digital rights and ownership: NFTs*. Retrieved from <https://digitalchamber.org/priorities/digital-rights-and-ownership/>
- [15] W3C Team. (2024, September 30). *Call for Participation in Blockchain2 Community Group*. Retrieved from <https://www.w3.org/community/bc2/2024/09/30/call-for-participation-in-blockchain2-community-group/>

## Annex 1

### Summary of Blockchain & DLT Publications

SDO	Publication	PA	INATBA Category (level 1)
<a href="#">ANSI</a>	<a href="#">ASC X9 Study Group Report Distributed Ledger and Blockchain Technology Study Group</a>	0	Technology
<a href="#">ANSI</a>	<a href="#">ANSI X9.138-2020 Distributed Ledger Technologies (DLT) Terminology</a>	0	Technology
<a href="#">ANSI</a>	<a href="#">ASC X9 TR 54-2021 Blockchain Risk Assessment Framework</a>	3	Security
<a href="#">DIN</a>	<a href="#">DIN SPEC 16597:2018-02 Terminology for blockchains</a>	0	Technology
<a href="#">DIN</a>	<a href="#">DIN SPEC 3104:2019-04 Blockchain-based validation of data</a>	2	Trust
<a href="#">DIN</a>	<a href="#">DIN SPEC 3103:2019-06 Blockchain and distributed ledger technologies in application scenarios for Industrie 4.0</a>	8	Technology
<a href="#">DIN</a>	<a href="#">DIN SPEC 4997:2020-04 Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology</a>	2	Security
<a href="#">DIN</a>	<a href="#">DIN SPEC 4996:2020-04 Blockchain-based approach to the transfer of software licenses</a>	8	Asset
<a href="#">DIN</a>	<a href="#">DIN/TS 31648:2021-04 Criteria for Trusted Transactions - Records Management and Evidence Retention in DLT and Blockchain</a>	2	Record
<a href="#">EEA</a>	<a href="#">EEA CIW - Crosschain Decentralization Guidelines Version 1.0</a>	5	Interoperability
<a href="#">EEA</a>	<a href="#">EEA CIW - Crosschain Interoperability Use Case Version 1.0</a>	6	Interoperability
<a href="#">EEA</a>	<a href="#">EEA CIW - Crosschain Security Guidelines Version 1.0</a>	7	Security
<a href="#">EEA</a>	<a href="#">EEA Client Specification Version 6</a>	0	System
<a href="#">ETSI</a>	<a href="#">ETSI GR IP6 031 V1.1.1 (2020-11) - IPv6 Security, Cybersecurity, Blockchain</a>	7	Security
<a href="#">ETSI</a>	<a href="#">ETSI GR IPE 012 V1.1.1 (2022-08) - IPv6 Enhanced innovation (IPE); IPv6-based Blockchain</a>	7	Technology

<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 001 V1.1.1 (2020-03) - Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies</a>	0	Technology
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 002 V1.1.1 (2020-11) - Permissioned Distributed Ledger (PDL); Applicability and compliance to data processing requirements</a>	3	Governance
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 003 V1.1.1 (2020-12) - Permissioned Distributed Ledger (PDL); Application Scenarios</a>	8	Technology
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 004 V1.1.1 (2021-02) - Permissioned Distributed Ledgers (PDL); Smart Contracts; System Architecture and Functional Specification</a>	6	Smart Contract
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 006 V1.1.1 (2022-08) - Permissioned Distributed Ledger (PDL); Inter-Ledger interoperability</a>	6	Interoperability
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 008 V1.1.1 (2021-09) - Permissioned Distributed Ledger (PDL); Research and Innovation Landscape</a>	6	Technology
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 009 V1.1.1 (2021-09) - Permissioned Distributed Ledger (PDL); Federated Data Management</a>	6	Governance
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 010 V1.1.1 (2021-08) - PDL Operations in Offline Mode</a>	5	System
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 014 V1.1.1 (2022-10) - Permissioned Distributed Ledger (PDL); Study on non-repudiation techniques</a>	7	Trust
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 018 V1.1.1 (2023-04) - Permissioned Distributed Ledger (PDL); Redactable Distributed Ledgers</a>	2	Ledger
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 019 V1.1.1 (2023-05) - PDL Services for Decentralized Identity and Trust Management</a>	1	Service
<a href="#">ETSI</a>	<a href="#">ETSI GR PDL 021 V1.1.1 (2023-10) - PDL; Use cases in 3GPP network</a>	8	Technology
<a href="#">ETSI</a>	<a href="#">ETSI GS PDL 011 V2.1.1 (2022-09) - Permissioned Distributed Ledger (PDL); Specification of Requirements for Smart Contracts' architecture and security</a>	7	Smart Contract
<a href="#">ETSI</a>	<a href="#">ETSI GS PDL 012 V1.2.1 (2023-06) - Permissioned Distributed Ledger (PDL); Reference Architecture</a>	0	System
<a href="#">ISO</a>	<a href="#">ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary</a>	0	Technology
<a href="#">ISO</a>	<a href="#">ISO 23257:2022 Blockchain and distributed ledger</a>	0	System

	<a href="#">technologies — Reference architecture</a>		
<a href="#">ISO</a>	<a href="#">ISO 24165-1:2021 Digital token identifier (DTI) — Registration, assignment and structure — Part 1: Method for registration and assignment</a>	4	Asset
<a href="#">ISO</a>	<a href="#">ISO 24165-2:2021 Digital token identifier (DTI) — Registration, assignment and structure — Part 2: Data elements for registration</a>	4	Asset
<a href="#">ISO</a>	<a href="#">ISO 8000-117:2023 Data quality — Part 117: Application of ISO 8000-115 to identifiers in distributed ledgers including blockchains</a>	2	Governance
<a href="#">ISO</a>	<a href="#">ISO/IEC TR 30176:2021 Internet of Things (IoT) — Integration of IoT and DLT/blockchain: Use cases</a>	8	Technology
<a href="#">ISO</a>	<a href="#">ISO/TR 23244:2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations</a>	7	Security
<a href="#">ISO</a>	<a href="#">ISO/TR 23249:2022 Blockchain and distributed ledger technologies — Overview of existing DLT systems for identity management</a>	1	System
<a href="#">ISO</a>	<a href="#">ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems</a>	5	Smart Contract
<a href="#">ISO</a>	<a href="#">ISO/TR 23576:2020 Blockchain and distributed ledger technologies — Security management of digital asset custodians</a>	7	Security
<a href="#">ISO</a>	<a href="#">ISO/TR 23644:2023 Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management</a>	1	Trust
<a href="#">ISO</a>	<a href="#">ISO/TR 24374:2023 Financial services — Security information for PKI in blockchain and DLT implementations</a>	7	Security
<a href="#">ISO</a>	<a href="#">ISO/TR 3242:2022 Blockchain and distributed ledger technologies — Use cases</a>	8	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T DSTN-IoT-DLT-Accounting - Accounting and billing aspects in Internet of Things (IoT) ecosystem and integrated approach using Distributed Ledger Technology (DLT)</a>	8	Service

<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.0 Requirements for distributed ledger systems</a>	0	System
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.1 Assessment criteria for distributed ledger technology platforms</a>	7	System
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.10 Framework and requirements for distributed ledger technology (DLT)-based digital collection services</a>	8	Service
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.11 Performance test suite for distributed ledger technology systems</a>	5	System
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.12 Formal verification framework for smart contract on distributed ledger technology</a>	6	Smart Contract
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.13 Framework and requirements for distributed ledger technology-based distributed power trading systems</a>	8	System
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.2 Reference framework for distributed ledger technologies</a>	0	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.3 Requirements for change management in distributed ledger technology (DLT)-based decentralized applications</a>	3	Governance
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.4 General framework for distributed ledger technology (DLT)-based invoices</a>	8	Asset
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.5 Requirements for distributed ledger technology-based power grid data management</a>	8	Governance
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.6 Performance assessment methods for distributed ledger technology platforms</a>	5	System
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.7 Functional assessment methods for distributed ledger technology platforms</a>	5	System
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.8 Technical framework for distributed ledger technology (DLT) to cope with regulation</a>	8	Governance
<a href="#">ITU-T</a>	<a href="#">ITU-T F.751.9 Trusted execution environment-based confidential computing on distributed ledger technology systems</a>	2	Security
<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D1.1 DLT terms and definitions</a>	0	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D1.2 DLT overview, concepts, ecosystem</a>	0	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D1.3 DLT standardization landscape</a>	0	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D2.1 DLT use cases</a>	8	Technology

<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D3.1 DLT reference architecture</a>	0	System
<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D3.3 Assessment criteria for DLT platforms</a>	7	System
<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D4.1 DLT regulatory framework</a>	8	Governance
<a href="#">ITU-T</a>	<a href="#">ITU-T FG DLT D5.1 Outlook on DLTs</a>	8	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T FG-AI4EE D.WG2-05 - Guidelines on energy efficient blockchain systems</a>	5	System
<a href="#">ITU-T</a>	<a href="#">ITU-T Technical Report D3.5 – Overview of blockchain for supporting IoT and SC&amp;C in DPM aspects</a>	5	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T Technical Specification D3.6 – Blockchain-based data exchange and sharing for supporting IoT and SC&amp;C</a>	5	Interoperability
<a href="#">ITU-T</a>	<a href="#">ITU-T Technical Specification D3.7 – Blockchain-based data management for supporting IoT and SC&amp;C</a>	5	Governance
<a href="#">ITU-T</a>	<a href="#">ITU-T Technical Specification D3.8 – Identity framework in blockchain to support DPM for IoT and SC&amp;C</a>	5	Trust
<a href="#">IEEE</a>	<a href="#">IEEE 2140.1-2020 IEEE Standard for General Requirements for Cryptocurrency Exchanges</a>	4	System
<a href="#">IEEE</a>	<a href="#">IEEE 2140.2-2021 IEEE Standard for Security Management for Customer Cryptographic Assets on Cryptocurrency Exchanges</a>	7	Security
<a href="#">IEEE</a>	<a href="#">IEEE 2140.4-2023 IEEE Standard for Distributed/Decentralized Exchange Framework using Distributed Ledger Technology (DLT)</a>	8	System
<a href="#">IEEE</a>	<a href="#">IEEE 2140.5-2020 IEEE Standard for a Custodian Framework of Cryptocurrency</a>	4	Asset
<a href="#">IEEE</a>	<a href="#">IEEE 2142.1-2021 IEEE Recommended Practice for E-Invoice Business Using Blockchain Technology</a>	8	Service
<a href="#">IEEE</a>	<a href="#">IEEE 2143.1-2020 IEEE Standard for General Process of Cryptocurrency Payment</a>	4	Service
<a href="#">IEEE</a>	<a href="#">IEEE 2144.1-2020 IEEE Standard for Framework of Blockchain-based Internet of Things (IoT) Data Management</a>	8	Governance
<a href="#">IEEE</a>	<a href="#">IEEE 2145-2023 - Practice for Blockchain Governance</a>	3	Governance
<a href="#">IEEE</a>	<a href="#">IEEE 2146.1-2022 IEEE Standard for Entity-Based Risk Mutual Assistance Model through Blockchain Technology</a>	3	Security
<a href="#">IEEE</a>	<a href="#">IEEE 2418.10-2022 IEEE Standard for Blockchain based Digital Asset Management</a>	8	Asset

<a href="#">IEEE</a>	<a href="#">IEEE 2418.2-2020 IEEE Standard for Data Format for Blockchain Systems</a>	2	Ledger
<a href="#">IEEE</a>	<a href="#">IEEE 2418.7-2021 IEEE Standard for the Use of Blockchain in Supply Chain Finance</a>	8	Service
<a href="#">IEEE</a>	<a href="#">IEEE 3205-2023 - Blockchain Interoperability Protocol</a>	0	Interoperability
<a href="#">IEEE</a>	<a href="#">IEEE 3207-2022 IEEE Standard for Blockchain-Based Digital Asset Identification</a>	8	Asset
<a href="#">NIST</a>	<a href="#">NISTIR 8202 Blockchain Technology Overview</a>	0	Technology
<a href="#">NIST</a>	<a href="#">NIST CSWP 9 A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems</a>	1	System
<a href="#">NIST</a>	<a href="#">NISTIR 8301 Blockchain Networks: Token Design and Management Overview</a>	4	Asset
<a href="#">NIST</a>	<a href="#">NISTIR 8419 Blockchain and Related Technologies to Support Manufacturing Supply Chain Traceability: Needs and Industry Perspectives</a>	8	Service
<a href="#">NIST</a>	<a href="#">NISTIR 8403 Blockchain for Access Control Systems</a>	8	Security
<a href="#">UNE</a>	<a href="#">UNE 71307-1:2020 Digital Enabling Technologies. Decentralised Identity Management Model based on Blockchain and other Distributed Ledgers Technologies. Part 1: Reference Framework</a>	1	Trust
<a href="#">EEA</a>	<a href="#">EEA DLT Interoperability Specification 1.0</a>	0	Interoperability
<a href="#">EEA</a>	<a href="#">EEA EthTrust Security Levels Specification Version 2.0</a>	7	Security
<a href="#">EEA</a>	<a href="#">EEA Off-Chain Trusted Compute Specification 1.0</a>	5	Trust
<a href="#">ETSI</a>	<a href="#">ETSI GS PDL 013 V1.1.1 (2022-10) - Permissioned Distributed Ledger (PDL); Supporting Distributed Data Management</a>	6	Governance
<a href="#">ETSI</a>	<a href="#">ETSI GS PDL 015 V1.1.1 (2023-01) - Permissioned Distributed Ledger (PDL); Reputation management</a>	1	Trust
<a href="#">ISO</a>	<a href="#">ISO/TR 6039:2023 Blockchain and distributed ledger technologies — Identifiers of subjects and objects for the design of blockchain systems</a>	8	System
<a href="#">ISO</a>	<a href="#">ISO/TR 6277:2024: Blockchain and distributed ledger technologies — Data flow models for blockchain and DLT use cases</a>	5	System
<a href="#">ISO</a>	<a href="#">ISO/TS 22739:2024 - Vocabulary</a>	0	Technology
<a href="#">ISO</a>	<a href="#">ISO/TS 23257:2022 - Reference architecture</a>	0	System



<a href="#">ISO</a>	<a href="#">ISO/TS 23258:2021 Blockchain and distributed ledger technologies — Taxonomy and Ontology</a>	0	Technology
<a href="#">ISO</a>	<a href="#">ISO/TS 23526:2023 - Security aspects for digital currencies</a>	7	Security
<a href="#">ISO</a>	<a href="#">ISO/TS 23576:2020 - Security of digital asset custodians</a>	7	Security
<a href="#">ISO</a>	<a href="#">ISO/TS 23635:2022 Blockchain and distributed ledger technologies — Guidelines for governance</a>	3	Governance
<a href="#">ITU-T</a>	<a href="#">ITU-T X.1400 (2020) - DLT terms and definitions</a>	0	Technology
<a href="#">ITU-T</a>	<a href="#">ITU-T X.1401 (2019) - Security threats to DLT</a>	7	Security
<a href="#">ITU-T</a>	<a href="#">ITU-T X.1402 (2020) - Security framework for DLT</a>	7	Security
<a href="#">ITU-T</a>	<a href="#">ITU-T X.1403 (2020) - Guidelines for decentralized identity</a>	1	Trust
<a href="#">ITU-T</a>	<a href="#">ITU-T X.1404 (2020) - Security assurance for DLT</a>	7	Security
<a href="#">ITU-T</a>	<a href="#">ITU-T X.1405 (2021) - Digital payment threats</a>	7	Security
<a href="#">ITU-T</a>	<a href="#">ITU-T X.1406 (2022) - Threats to online voting using DLT</a>	8	Security
<a href="#">IEEE</a>	<a href="#">IEEE 3209-2023 - Blockchain Identity Key Management</a>	1	Security
<a href="#">IEEE</a>	<a href="#">IEEE 3218-2022 IEEE Standard for Using Blockchain for Carbon Trading Applications</a>	8	Service
<a href="#">IEEE</a>	<a href="#">IEEE 3224-2023 - Green Power Identification</a>	8	Asset
<a href="#">IEEE</a>	<a href="#">IEEE 3801-2022 IEEE Standard for Blockchain-based Electronic Contracts</a>	8	Smart Contract
<a href="#">IEEE</a>	<a href="#">IEEE 3802-2022 IEEE Standard for Application Technical Specification of Blockchain-based E-Commerce Transaction Evidence Collecting</a>	8	Record
<a href="#">NIST</a>	<a href="#">NISTIR 8408 (2023-09) - Stablecoin Security Considerations</a>	4	Security

## Annex 2

List of all finalized ERC standards

Number	Title	Number	Title
<a href="#">20</a>	Token Standard	<a href="#">5267</a>	Retrieval of EIP-712 domain

Number	Title	Number	Title
<a href="#"><u>55</u></a>	Mixed-case checksum address encoding	<a href="#"><u>5313</u></a>	Light Contract Ownership
<a href="#"><u>137</u></a>	Ethereum Domain Name Service - Specification	<a href="#"><u>5375</u></a>	NFT Author Information and Consent
<a href="#"><u>162</u></a>	Initial ENS Hash Registrar	<a href="#"><u>5380</u></a>	ERC-721 Entitlement Extension
<a href="#"><u>165</u></a>	Standard Interface Detection	<a href="#"><u>5484</u></a>	Consensual Soulbound Tokens
<a href="#"><u>173</u></a>	Contract Ownership Standard	<a href="#"><u>5489</u></a>	NFT Hyperlink Extension
<a href="#"><u>181</u></a>	ENS support for reverse resolution of Ethereum addresses	<a href="#"><u>5507</u></a>	Refundable Tokens
<a href="#"><u>190</u></a>	Ethereum Smart Contract Packaging Standard	<a href="#"><u>5521</u></a>	Referable NFT
<a href="#"><u>191</u></a>	Signed Data Standard	<a href="#"><u>5528</u></a>	Refundable Fungible Token
<a href="#"><u>223</u></a>	Token with transaction handling model	<a href="#"><u>5564</u></a>	Stealth Addresses
<a href="#"><u>600</u></a>	Ethereum purpose allocation for Deterministic Wallets	<a href="#"><u>5570</u></a>	Digital Receipt Non-Fungible Tokens
<a href="#"><u>601</u></a>	Ethereum hierarchy for deterministic wallets	<a href="#"><u>5585</u></a>	ERC-721 NFT Authorization
<a href="#"><u>681</u></a>	URL Format for Transaction Requests	<a href="#"><u>5606</u></a>	Multiverse NFTs
<a href="#"><u>721</u></a>	Non-Fungible Token Standard	<a href="#"><u>5615</u></a>	ERC-1155 Supply Extension
<a href="#"><u>777</u></a>	Token Standard	<a href="#"><u>5625</u></a>	NFT Metadata JSON Schema dStorage Extension
<a href="#"><u>820</u></a>	Pseudo-introspection Registry Contract	<a href="#"><u>5646</u></a>	Token State Fingerprint
<a href="#"><u>1046</u></a>	tokenURI Interoperability	<a href="#"><u>5679</u></a>	Token Minting and Burning

Number	Title	Number	Title
<a href="#">1155</a>	Multi Token Standard	<a href="#">5725</a>	Transferable Vesting NFT
<a href="#">1167</a>	Minimal Proxy Contract	<a href="#">5732</a>	Commit Interface
<a href="#">1271</a>	Standard Signature Validation Method for Contracts	<a href="#">5750</a>	General Extensibility for Method Behaviors
<a href="#">1328</a>	WalletConnect URI Format	<a href="#">5773</a>	Context-Dependent Multi-Asset Tokens
<a href="#">1363</a>	Payable Token	<a href="#">6059</a>	Parent-Governed Nestable Non-Fungible Tokens
<a href="#">1820</a>	Pseudo-introspection Registry Contract	<a href="#">6066</a>	Signature Validation Method for NFTs
<a href="#">1967</a>	Proxy Storage Slots	<a href="#">6105</a>	No Intermediary NFT Trading Protocol
<a href="#">2098</a>	Compact Signature Representation	<a href="#">6147</a>	Guard of NFT/GBT, an Extension of ERC-721
<a href="#">2135</a>	Consumable Interface (Tickets, etc)	<a href="#">6150</a>	Hierarchical NFTs
<a href="#">2309</a>	ERC-721 Consecutive Transfer Extension	<a href="#">6220</a>	Composable NFTs utilizing Equippable Parts
<a href="#">2535</a>	Diamonds, Multi-Facet Proxy	<a href="#">6239</a>	Semantic Soulbound Tokens
<a href="#">2612</a>	Permit Extension for EIP-20 Signed Approvals	<a href="#">6381</a>	Public Non-Fungible Token Emote Repository
<a href="#">2678</a>	Revised Ethereum Smart Contract Packaging Standard (EthPM v3)	<a href="#">6454</a>	Minimal Transferable NFT detection interface
<a href="#">2771</a>	Secure Protocol for Native Meta Transactions	<a href="#">6492</a>	Signature Validation for Predeploy Contracts
<a href="#">2981</a>	NFT Royalty Standard	<a href="#">6538</a>	Stealth Meta-Address Registry
<a href="#">3156</a>	Flash Loans	<a href="#">6672</a>	Multi-redeemable NFTs

Number	Title	Number	Title
<a href="#">3448</a>	MetaProxy Standard	<a href="#">6808</a>	Fungible Key Bound Token
<a href="#">3475</a>	Abstract Storage Bonds	<a href="#">6809</a>	Non-Fungible Key Bound Token
<a href="#">3525</a>	Semi-Fungible Token	<a href="#">6982</a>	Efficient Default Lockable Tokens
<a href="#">3643</a>	T-REX - Token for Regulated EXchanges	<a href="#">7007</a>	Verifiable AI-Generated Content Token
<a href="#">3668</a>	CCIP Read—Secure offchain data retrieval	<a href="#">7053</a>	Interoperable Digital Media Indexing
<a href="#">4400</a>	EIP-721 Consumable Extension	<a href="#">7066</a>	Lockable Extension for ERC-721
<a href="#">4519</a>	Non-Fungible Tokens Tied to Physical Assets	<a href="#">7092</a>	Financial Bonds
<a href="#">4626</a>	Tokenized Vaults	<a href="#">7160</a>	ERC-721 Multi-Metadata Extension
<a href="#">4804</a>	Web3 URL to EVM Call Message Translation	<a href="#">7201</a>	Namespaced Storage Layout
<a href="#">4834</a>	Hierarchical Domains	<a href="#">7208</a>	On-Chain Data Containers
<a href="#">4906</a>	EIP-721 Metadata Update Extension	<a href="#">7231</a>	Identity-aggregated NFT
<a href="#">4907</a>	Rental NFT, an Extension of EIP-721	<a href="#">7401</a>	Parent-Governed Non-Fungible Tokens Nesting
<a href="#">4910</a>	Royalty Bearing NFTs	<a href="#">7409</a>	Public Non-Fungible Tokens Emote Repository
<a href="#">4955</a>	Vendor Metadata Extension for NFTs	<a href="#">7432</a>	Non-Fungible Token Roles
<a href="#">5006</a>	Rental NFT, NFT User Extension	<a href="#">7439</a>	Prevent ticket touting
<a href="#">5007</a>	Time NFT, ERC-721 Time Extension	<a href="#">7528</a>	ETH (Native Asset) Address

Number	Title	Number	Title
			Convention
<a href="#">5023</a>	Shareable Non-Fungible Token	<a href="#">7535</a>	Native Asset ERC-4626 Tokenized Vault
<a href="#">5169</a>	Client Script URI for Token Contracts	<a href="#">7540</a>	Asynchronous ERC-4626 Tokenized Vaults
<a href="#">5192</a>	Minimal Soulbound NFTs	<a href="#">7575</a>	Multi-Asset ERC-4626 Vaults
<a href="#">5202</a>	Blueprint contract format	<a href="#">7578</a>	Physical Asset Redemption
<a href="#">5219</a>	Contract Resource Requests	<a href="#">7588</a>	Blob Transactions Metadata JSON Schema
<a href="#">7818</a>	Expirable ERC-20	<a href="#">7734</a>	Decentralized Identity Verification (DID)
<a href="#">7820</a>	Access Control Registry	<a href="#">7751</a>	Wrapping of bubbled up reverts