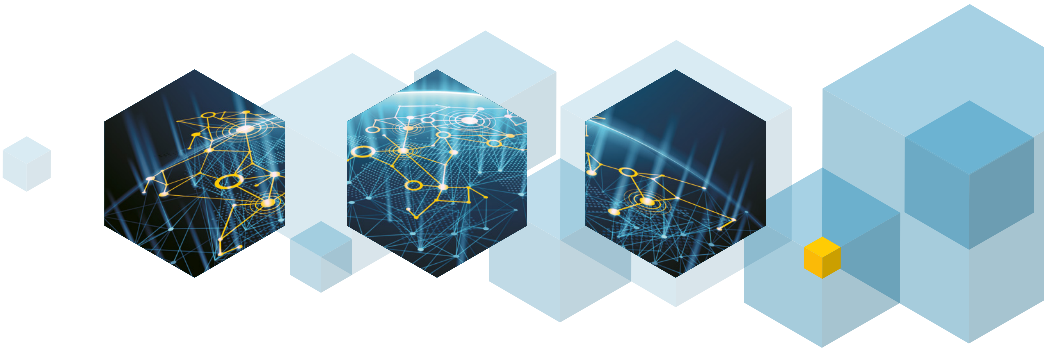
BLOCKCHAIN AND DISTRIBUTED LEDGERS

NATIONAL TECHNICAL STANDARDIZATION REPORT

Version 1.0 · June 2021

ISBN : 978-99987-869-0-5



BLOCKCHAIN AND DISTRIBUTED LEDGERS

NATIONAL TECHNICAL STANDARDIZATION REPORT

Version 1.0 · June 2021

ILNAS

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

ANEC

Agence pour la Normalisation et
l'Economie de la Connaissance

Foreword

Blockchains, and more generally Distributed Ledgers, have taken the Information and Communication Technologies (ICT) world by storm since the advent of the first worldwide decentralized cryptocurrency back in 2008. Over the last decade and a half, these techniques and concepts have been imagined as a novel way to better distribute trust across stakeholders within a complex system underlying applications far beyond an implementation of digital, decentralized cash: supply chains, financial instruments, data sharing, etc. Yet, challenges pertaining to scalability, governance, interoperability, security, and ultimately trust, remain, and need to be properly addressed to really make blockchains useful and mainstream.

Technical standardization plays an important part in the uptake of novel technologies, and this is no different for distributed ledgers. In the Grand Duchy of Luxembourg, the *"Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services"* (ILNAS) leads the implementation of the "Luxembourg Standardization Strategy 2020-2030"[1], signed by the Minister of the Economy, which identifies the ICT sector as one of the most relevant for national economic growth, along with the Construction and Aerospace sectors. ILNAS has also developed, in line with this strategy, the "Luxembourg's policy on ICT technical standardization 2020-2025"[2], which it carries out with the support of the Economic Interest Group *"Agence pour la Normalisation et l'économie de la Connaissance"* (ANEC GIE – Standardization Department). This policy places an emphasis on Smart ICT technologies such as Artificial Intelligence, Blockchain, Cloud Computing, and the Internet of Things, with the aim to promote and strengthen the use of technical standards by the national market, to reinforce the position of Luxembourg in the global ICT standardization landscape - particularly through a stronger involvement of national stakeholders in the relevant standardization technical committees - and to pursue the development of research and education programs in Smart ICT standardization.

In this context, and in collaboration with the University of Luxembourg, ILNAS has created a new Master's degree "Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions"[3], that started in February 2021. This diploma has the aim to allow national stakeholders to discover Smart Secure ICT, including Blockchain and Distributed Ledger Technology, notably from a standardization and Technopreneurship point of view, in order to seize the future business opportunities offered in this innovative area.

ILNAS has also launched, and worked on, various research activities in Smart Secure ICT, which directly contribute to the success of its program on standardization education. As a result, multiple deliverables have been produced. In collaboration with the University of Luxembourg, a white paper "Data Protection and Privacy in Smart ICT"[4] and three technical reports on the gaps between scientific research and technical standardization in Cloud Computing, Internet of Things and Big Data/Artificial Intelligence[5] were published in October 2018 and October 2019, respectively. More publications were realized with the support of the ANEC GIE in order to inform the market about technical standardization

[1] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-luxembourgeoise-2020-2030.html

[2] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2020-2025.html

[3] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/education-normalisation.html

[4] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-data-protection-privacy-smart-ict.html

[5] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/technical-reports-gap-analysis-between-scientific-research-and-technical-standardization.html

developments in Smart ICT, such as the white papers on "Artificial Intelligence"[6], "Internet of Things"[7], or "Blockchain and Distributed Ledger Technologies"[8], as well as the technical report on "Internet of Things"[9].

This technical report is a follow-up on the "Blockchain" white paper from 2018. It is intended to further inform the national market about relevant Blockchain and Distributed Ledger Technology standardization activities and opportunities, with a view towards encouraging the national market's involvement in the standards development process, for the benefit of Luxembourg's economy.

Jean-Marie REIFF
Director
ILNAS

Jean-Philippe HUMBERT
Deputy Director
ILNAS

[6] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-artificial-intelligence-and-technical-standardization.html

[7] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-iot.html

[8] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-blockchain-dlt.html

[9] https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/national-technical-standardization-report-iot-june-2020.html

Acknowledgements

The working group involved in the preparation of this technical report is:

Name of the contributor	Institution/Organization
Mr. Jean-Marie REIFF	ILNAS
Dr. Jean-Philippe HUMBERT	ILNAS
Mr. Nicolas DOMENJOUD	ILNAS
Mrs. Leslie FOUQUERAY	ANEC GIE
Dr. Jean LANCRENON	ANEC GIE

Table of contents

Abbreviations

AI	Artificial Intelligence
ANEC GIE	*Agence pour la Normalisation et l'Economie de la Connaissance*
BFT	Byzantine Fault Tolerance
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
DAG	Directed Acyclic Graph
DL	Distributed Ledger
DLT	Distributed Ledger Technology
EBSI	European Blockchain Service Infrastructure
EC	European Commission
EEA	Enterprise Ethereum Alliance
ETSI	European Telecommunications Standards Institute
EU	European Union
ICO	Initial Coin Offering
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEEE SA	IEEE Standards Association
ILNAS	*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*
INATBA	International Association for Trusted Blockchain Applications
IOHK	Input Output Hong Kong
IoT	Internet of Things
IS	International Standard
ISG	Industry Specification Group
ISO	International Organization for Standardization
ITU	International Telecommunications Union
ITU-T	ITU's Telecommunication standardization sector
IWA	The InterWork Alliance
NIST	National Institute of Standards and Technology
PBFT	Practical Byzantine Fault Tolerance
PDL	Permissioned Distributed Ledger
SDO	Standards Developing Organization
SG	Study Group
TC	Technical Committee
TR	Technical Report
TS	Technical Specification
XRP	Ripple currency denomination

List of Figures

List of Tables

Introduction

Blockchains, and more generally Distributed Ledger Technologies (DLT), have now been touted for close to 15 years as the future of collaborative Information and Communication Technologies (ICT) across potentially mutually distrusting parties. However, their adoption has been fraught with difficulty, owing to their complexity, a hype that is sometimes exaggerated, and even bad press stemming for instance from Initial Coin Offerings (ICOs) bordering on fraud, wherein the promise of an imaginary solution has translated sometimes into very real losses in investments. Technical challenges also abound, ranging from scalability all the way to decentralized and inter-organizational governance, and going through interoperability, not just between blockchains, but also with legacy systems.

Yet, the promise of a bright future for DLT remains strong, and is worth pursuing, especially as the world becomes ever more digitized. ICT collaboration, the sharing of systems and data, the creation of more and more connections via, for instance, the Internet of Things (IoT), the pooling of compute power through the Cloud, and far-reaching analyses performed by agents of Artificial Intelligence (AI) all make up a growing landscape where decentralization will eventually become the norm and not the exception. This makes the fair distribution of trust in systems, which blockchains and distributed ledgers can help achieve, all the more significant. Thus, the effort to stabilize and encourage the uptake of these technologies has value.

Part of the process lies with technical standardization. The agreement upon, drafting, and publishing of baseline requirements and good practices are paramount to get all actors involved in the industry on the same page, in order to improve technology, foster adoption, and yield benefits for all. These are foundational concepts in technical standardization, and Luxembourg's market can have its say in the process by getting involved. With this report, which is a follow-up of ILNAS' white paper on Blockchain technologies from 2018 [1], the aim is to keep stakeholders of the economy informed on the latest Blockchain standards developments of relevance to their business. It is one deliverable among many, in the overall effort put forward by ILNAS with the support of the ANEC GIE to lead the implementation of the 2020-2030 National Standardization Strategy[10].

The report is structured as follows:

- Chapter 1 is an overview of the concepts that underpin Blockchain technology,
- Chapter 2 details a few examples of what one can find in the Blockchain technology landscape,
- Chapter 3 gives pointers on key Blockchain initiatives and overviews potential applications, and
- Chapter 4 shows the state of the Blockchain and DLT standardization landscape, and how one can get involved in technical standardization activities in Luxembourg.

It is our hope that the reader gains insight from this document, especially with a view towards participating in shaping the standardization future of this important new set of technologies.

[10] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-luxembourgeoise-2020-2030.html

1

Distributed Ledger Technology – A conceptual overview

1. Distributed Ledger Technology – A conceptual overview

In this chapter, we give an overview of the main concepts underlying distributed ledgers. There are essentially two of these: 1) how mutually distrustful parties agree collectively on the value of a database, and 2) how to automatically execute computerized, distributed contracts in a trusted way. The latter concept builds on the former.

1.1. The concept of collectively maintained ledgers

1.1.1. Principles

Ledgers

A ledger is an account of a system's history over a certain time period. It regularly records new entries on the state of this system as the system evolves. Ideally, the ledger should be considered immutable in order for meaningful comparisons to be made between recorded states at two points in time. Indeed, if the ledger can be altered at will, it is trivial to make the system's history consistent with statements made in the present. The historical ledger example is the account of a company's finances, regularly audited, e.g. for tax or anti-money-laundering purposes[11].

Clearly, control over a ledger is a delicate affair. On the one hand, the main stakeholder in a ledger's content should not be in sole control over it, lest it decide to re-write it for a more convenient narrative at audit time. On the other hand, one may not want to fully outsource a ledger's control to a third party, since this means placing an exaggerated amount of trust in that very party.

Distributing the rights to ledger editing

What is needed is a way for multiple parties with a stake in the ledger's contents to distribute the *writing-rights* among themselves in a fair way. In particular, they should be able to completely eliminate the need for a trusted third party to serve as an adjudicator.

We make the assumption that at any given time all parties have a copy of the ledger in a certain state. What they have to agree on every now and then is whether a proposed change to this state – *a transaction* – is accepted or not. If yes, the ledger is updated accordingly for everybody. If not, the transaction is simply rejected. In either case, all ledger copies are synchronized. We also assume that transactions are broadcast to all parties involved. The parties may be connected with one another only remotely, for instance through the Internet. Finally, it is assumed that parties that act maliciously can do so by *deviating arbitrarily* from the specified protocol.

[11] https://www.investopedia.com/terms/g/generalledger.asp (accessed 22/03/2021)

Distributed ledgers and blockchains

A distributed ledger (DL) is a ledger replicated at each stakeholder's location and to which proposed modifications and updates are collectively agreed to by these stakeholders, see Figure 1.

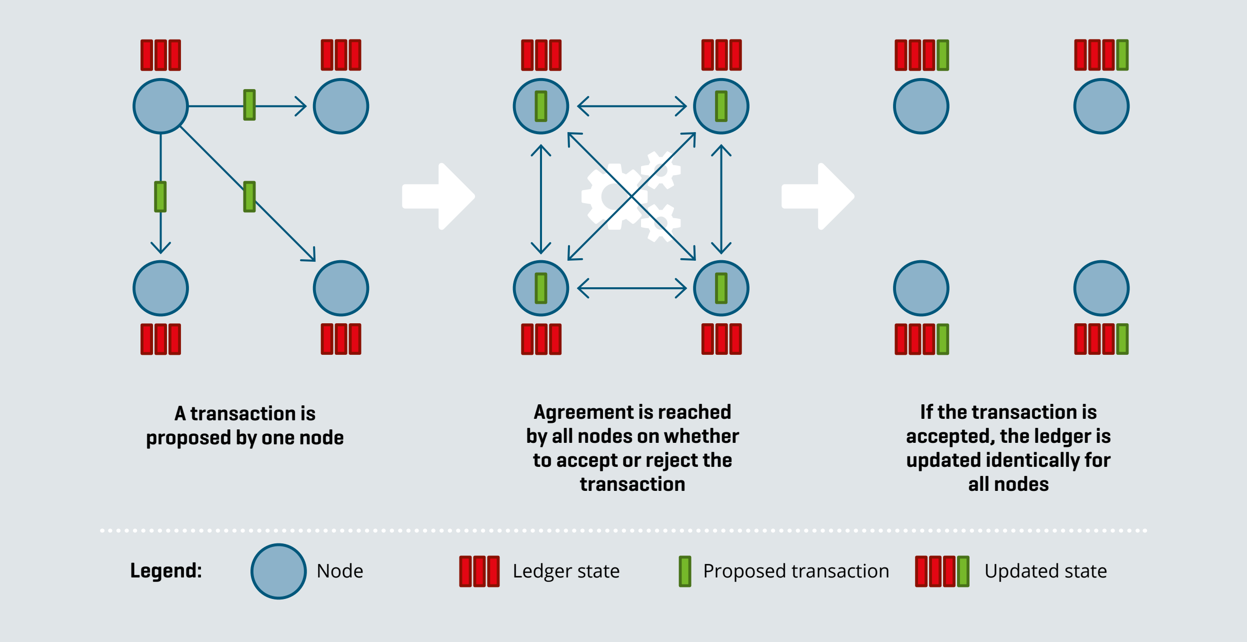
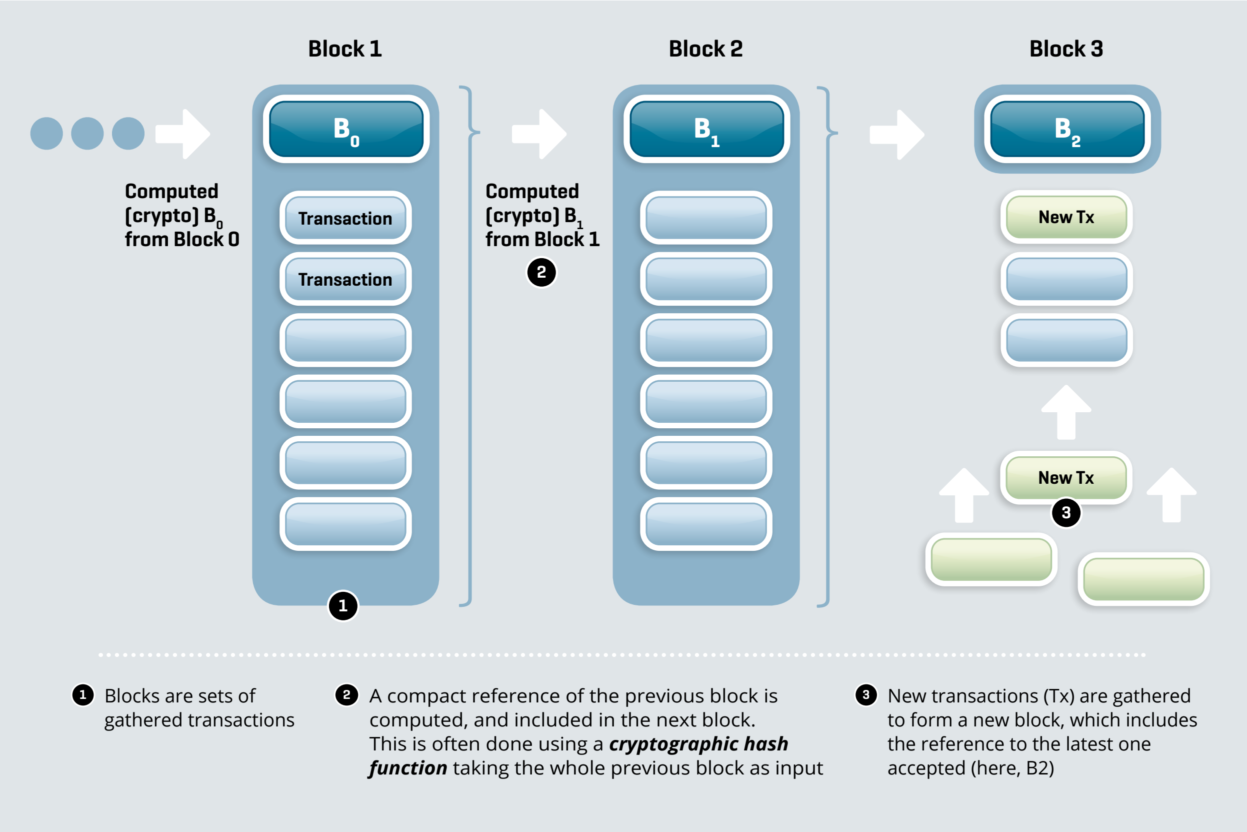

A transaction is proposed by one node
Agreement is reached by all nodes on whether to accept or reject the transaction
If the transaction is accepted, the ledger is updated identically for all nodes
Legend:
Node
Ledger state
Proposed transaction
Updated state

Figure 1: Distributed ledger between four nodes

A blockchain is a specific type of distributed ledger wherein the ledger data consists in a growing sequence of groups of transactions validated by a *consensus mechanism*, each such group being *cryptographically embedded* into the next, forming a totally ordered chain of transaction-filled blocks. Nodes that run the consensus mechanism on input a selected group of eligible transactions are typically called *miners*. In a blockchain structure, honest miners will continue mining over the last block of the chain that has received the most work (which is usually the longest one identified). Each round of voting creates a new block, see Figure 2.

The overall set of DL techniques and concepts is known as Distributed Ledger Technology (DLT).



❶ Blocks are sets of gathered transactions

❷ A compact reference of the previous block is computed, and included in the next block. This is often done using a ***cryptographic hash function*** taking the whole previous block as input

❸ New transactions (Tx) are gathered to form a new block, which includes the reference to the latest one accepted (here, B2)

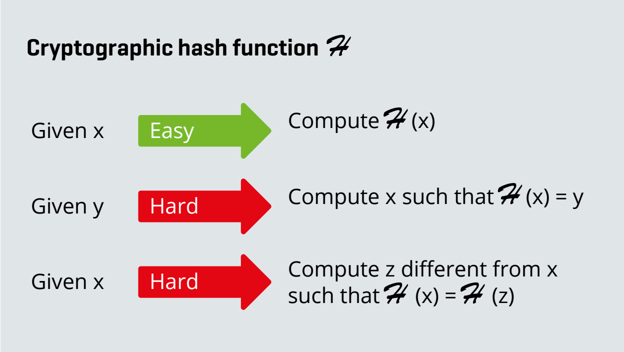
Figure 2: Creating and chaining blocks

It is important to keep in mind that while blockchains are distributed ledgers, not all distributed ledgers are structured as blockchains[12].

The cryptography used in blockchains

The two most important cryptographic algorithms that are used in blockchains and DLT are cryptographic hash functions and digital signatures.

A hash function is a mathematical function that takes an input of arbitrary size and computes an output of some pre-fixed length (in bits). A hash function is said to be cryptographic if it is easy to compute but computationally hard (that is, infeasible) to invert and hard to find collisions for. Hashing a block and embedding the result in the subsequent one makes it infeasible for adversaries to substitute a previously validated block with a different one, because the "bad" block would have to hash to the reference of the one it aims to replace, and this constitutes a collision on the function.


Cryptographic hash function $\mathcal{H}$
Given x
Easy
Compute $\mathcal{H}$ (x)
Given y
Hard
Compute x such that $\mathcal{H}$ (x) = y
Given x
Hard
Compute z different from x such that $\mathcal{H}$ (x) = $\mathcal{H}$ (z)

[12] The IOTA distributed ledger [23], which we will cover in more detail in Chapter 2, is organized as a directed acyclic graph of transactions.

A digital signature is an algorithm that allows a holder of a private key to digitally sign electronic information. The private key has a corresponding public key, with which anybody wishing to verify the electronic signature can do so. Thus, provided the private key remains in sole custody of its rightful owner, information signed in this way is cryptographically bound to that owner.

Definitional foundations in standards

Blockchains and DLT are extremely recent inventions, dating only as far back as 2008 with the publication of the seminal paper describing Bitcoin [2]. A little over a decade later, they are at the center of a global hype and ecosystem that many are willing to consider the advent of a technological revolution[13]. In order to advance adoption and interoperability coherently on a worldwide scale, there first needs to be some global effort to answer the question: "What are these objects?"

This is exactly the starting point of any technical standardization process. In the technical committee ISO/TC 307 *Blockchain and Distributed ledger technologies*[14], Working Group 1 *Foundations* has this task. It has namely published an international standard on terminology (ISO 22739:2020 *Blockchain and distributed ledger technologies — Vocabulary*[15]), and is currently working on an international standard describing a reference architecture (ISO 23257 *Blockchain and distributed ledger technologies — Reference architecture*[16]), and a technical specification to classify various objects of the Blockchain ecosystem (ISO/TS 23258 *Blockchain and distributed ledger technologies — Taxonomy and Ontology*[17]). More information on standardization can be found in Chapter 4.

1.1.2. Establishing consensus

We make the distinction between *closed systems* and *open systems*. In a closed system, there is a pre-fixed groups of nodes that are all known to each other in advance, and that communicate with one another in an authenticated way. In contrast, an open system is one that parties may leave or join at will, and within which they may be anonymous (or at least, pseudonymous).

Historically, consensus mechanisms between nodes have been studied for quite some time (see for instance [3]), but only in the closed-system case. Classically, algorithms for this are called *Byzantine Fault Tolerance* (BFT) protocols. With the Bitcoin white paper from 2008 [2], the case of open systems was first considered, and the new class of protocols that result from it are named *Nakamoto consensus protocols*. While the latter class is newer and arguably a hotter topic, both classes have their strengths and weaknesses, and their own place in the DLT ecosystem. Furthermore, the advent of research into open systems has also re-invigorated interest and research into protocols for closed ones [4].

Byzantine fault tolerance

The problem of basic fault tolerance – in which a group of nodes must reach consensus despite a number of them *simply failing* – was first considered in [5], and are interesting in their own right. A more modern protocol for this setup is Paxos [6]; it achieves consensus with at most f faulty nodes where $n=2f+1$, n being the total number of nodes.

[13] "You can't stop things like Bitcoin. It will be everywhere and the world will have to readjust. World governments will have to readjust"- John McAfee, Founder of McAfee. "What the internet did for communications, I think blockchain will do for trusted transactions." – Ginni Rometty, CEO of IBM.

[14] https://www.iso.org/committee/6266604.html

[15] https://www.iso.org/standard/73771.html?browse=tc

[16] https://www.iso.org/standard/75093.html?browse=tc

[17] https://www.iso.org/standard/75094.html?browse=tc

The more complicated case of BFT – wherein nodes can behave in arbitrary malicious ways - was first considered by Lamport et al. in [3].

BFT protocols are deterministic, in that as long as a threshold of malicious players is not surpassed, running the algorithm will always result in the outcome favored by the honest participants. BFT is not scalable in the number of nodes, but is scalable in transaction throughput. The most widely known protocol for BFT is *Practical Byzantine Fault Tolerance* (PBFT, [7]). Honest consensus will be achieved as long as there are only up to f adversarial nodes, where the total number n of nodes verifies $n=3f+1$. PBFT is essentially the basis of most BFT protocols that are considered today.

Nakamoto consensus

In a setting as general as an open system, a direct election on a transaction's acceptability - wherein votes are counted, say, by username in some pre-agreed online system, or even by IP address - is simply not robust enough. It is too easy for a given party to mount a *Sybil* attack, where it masquerades as many different voters to bias the election, in an effort to get its way[18].

The real technical challenge in this case is to *constrain voting power* by making it a function of some resource that is impractical or costly to increase by a node. This is exactly what Nakamoto consensus mechanisms are designed for. What varies from method to method is the resource considered.

Proof-of-work

This is by far the most used and known Nakamoto consensus method. In proof-of-work, the transaction-validating party is the first to broadcast a solution to a hard-to-solve, yet easy-to-verify computational puzzle. At each new round of voting, a fresh puzzle instance is generated for all miners to work on, in order to keep malicious voters from pre-computing solutions. The point is to make voting power proportional to *owned computational power* (hence the expression "one PC, one vote", [2]).

Systems that use proof-of-work include Bitcoin and Ethereum [8]. Proof-of-work's most obvious drawback is its power consumption (see for instance [9], which places the annual mining energy consumption for Bitcoin on par with the annual energy consumption of Argentina).

Proof-of-stake

Proof-of-stake makes voting power a function of the *resources a given miner holds* in the system, that is, how much stake that miner has invested. On the one hand, this favors resource-plentiful participants, but on the other hand, the value of these resources is only guaranteed as long as the system functions properly. Hence, "wealthy" participants are incentivized to behave according to system specifications.

Peercoin [10] uses such a consensus mechanism, and Ethereum has an ongoing project to migrate from proof-of-work to proof-of-stake [11]. A main drawback to proof-of-stake is that it suffers from the so-called *nothing-at-stake* problem [4]: since mining is easy, participants are tempted to mine over many possible concurrent chains to be sure that they "choose" the right one for their next block, leading to forks (see Section 1.1.3.).

[18] https://en.wikipedia.org/wiki/Sybil_attack (accessed 22/03/2021)

Proof-of-space

Proof-of-space [12] gives more voting power to miners dedicating more *storage capacity* to the system. The main underlying idea is to have the voting party generate a large volume of specially structured data that can be probed at arbitrary locations at election time to prove the occupation of space. Advantages include the fact that space is a reusable resource and that investing in disk space is a one-off event (in contrast, e.g., to electricity costs of proof-of-work mining).

Burstcoin [13] and Spacemint [14] use this sort of consensus. Proof-of-space, like proof-of-stake, suffers also from the *nothing-at-stake* problem [4].

It is important to emphasize that Nakamoto consensus methods are, in contrast to BFT, only *probabilistic*. That is, only with a certain success probability will the honest decision win. However, the longer a working blockchain implementing Nakamoto consensus grows, the lower the probability that a confirmed transaction will be removed gets, and this occurs at an exponential rate [15]. This is because the speed at which honest blocks accumulate on average will always be greater than that at which dishonest blocks accumulate, resulting in the honest chain being the main one attracting honest participants with an overwhelming chance.

Finally, similarly to BFT, Nakamoto consensus methods operate based on the assumption that *malicious players collectively control only a bounded fraction of the resource underlying the consensus mechanism*. Exactly how large this fraction can be is much more difficult to evaluate than with BFT, precisely because the outcome is no longer deterministic. As an example, initially it was believed that Bitcoin was safe assuming the adversary controls no more than 49% of the total computational resources, see [2]. However, research (see for instance [16]) has shown that the threshold could really be more around 25%, which is considerably less[19].

Hybrid consensus methods

Hybrid consensus methods attempt to get the best of both worlds, in a two-tiered process. They will typically use a proof-of-X method to form one or more temporary committees of validating nodes, which only then use a more efficient Byzantine consensus method to validate transactions. Care must be taken to not have inconsistent transaction information between these committees. One example of a protocol designed to function like this is Elastico [17].

1.1.3. Trust architectures

Permissions

There are basically two trust architectures for distributed ledgers: the permissioned architecture is that of a closed system, while the permissionless one is that of an open system; both of these were described in Section 1.1.2.

Note that permissioned systems can only work if there is an external governance system in place to control node participation. This governance can either come in the form of a consortium or a single entity.

[19] The problem of designing a framework for satisfactory evaluation of Nakamoto consensus is open, and under investigation, see [69].

Governance

The main challenge in governance of a DLT system is to not negate technically achieved disintermediation through an underlying set of off-chain rules. It is clear that such rules must always exist, as even at the software development level, core developers must agree on the code to update and distribute. This is particularly true in the case of public, permissionless chains (e.g. Bitcoin or Ethereum).

The governance system for the base software of Ethereum is a completely off-chain system, based on open discussions between the core software developer team and users of the system. Having an open process is fundamental because ultimately any change to the base code must be very widely accepted in order to avoid costly hard forks [18][20]. However, the process remains largely loose and informal.

Some research suggests that a type of formal governance will eventually emerge for stability reasons. In [19], it is argued that mining fees for Bitcoin will not be enough to maintain the system in case once mining rewards vanish (due to the pre-fixed supply of currency), at least if transaction fees are not made mandatory. Yet, such a decision requires off-chain consensus in the Bitcoin community, in particular in the core developer team, and it is hard to fathom such a massive change being brought through an informal process.

Standardization efforts in governance

It is well-known that technical standardization concerns *processes* as much as it does techniques and products. Accordingly, processes for good governance are the subject of attention from SDOs. In ISO/TC 307, WG 5 *Governance* is currently drafting a Technical Specification (ISO/TS 23635 *Blockchain and distributed ledger technologies — Guidelines for governance*[21]) to aid in clarifying what constitutes appropriate governance schema for various Blockchain or DLT settings. The specification covers both permissioned and permissionless systems.

1.2. Decentralized and automated contracts

1.2.1. History and purpose

The notion of a "smart contract" was first described by cryptographer Nick Szabo in [20]. His main idea was to use the modern age's new capabilities resulting from internet connectivity, digitization of documents, programmability of algorithms, and advanced cryptography to *digitize contracts* in an effort to reduce contractual transaction costs. These include many of the costs incurred by verifying that the contract is properly executed, especially enforcing its clauses.

It took the arrival, over a decade later, of distributed ledgers to finally have an adequate platform over which truly decentralized computing could be built. Indeed, automating a contract by running it as code on a computer is easy; but now one must select *whose computer to trust* to run that code on.

[20] In fact, a governance disagreement on how to handle a large-scale theft of ether (Ethereum's native cryptocurrency) due to a bug in the code led to there now being two versions of Ethereum, the second named Ethereum Classic [17] [72].

[21] https://www.iso.org/standard/76480.html?browse=tc

1.2.2. Smart contracts run over distributed ledgers

On a high level, using a DL to provide a trust-spreading environment over which decentralized computing works can be described as follows:

1. In a DLT system, a smart contract exists as a piece of code that is recorded in the ledger as a transaction. Thus, all participating nodes have a copy of the code, see Figure 3 (the "consensus running" part described in Figure 1 is implicit)

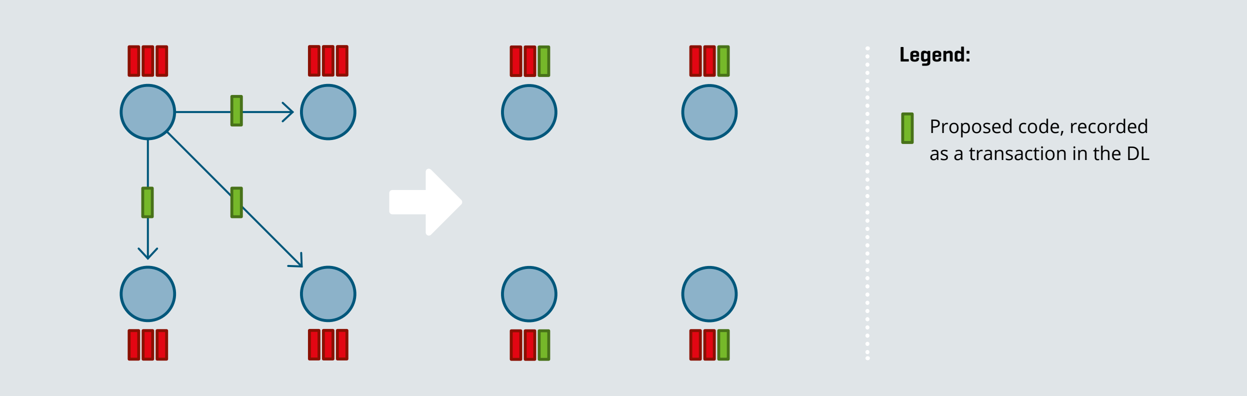


Figure 3: Smart contract recorded in the distributed ledger

2. If a node involved in the contract wishes to execute that contract, it records, again as a transaction, the necessary input in the DL. All other nodes see the input, and locally execute the code, see Figure 4.

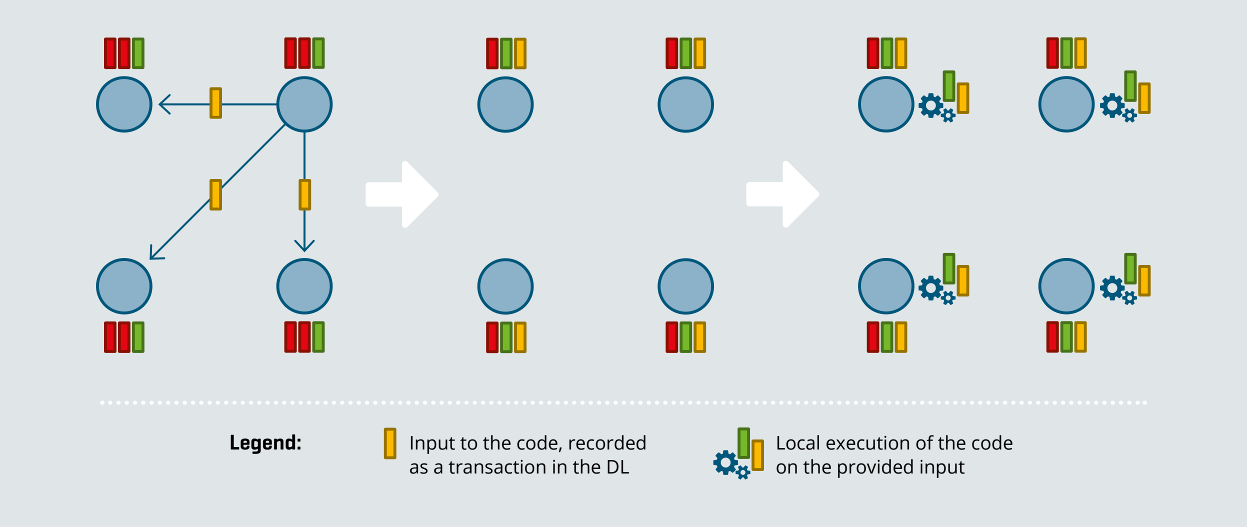

Legend:
Input to the code, recorded as a transaction in the DL
Local execution of the code on the provided input

Figure 4: Input to a smart contract recorded in the distributed ledger

3. Once the code is fully executed by a node, the output is recorded on the DL, see Figure 5. This will only occur if the output is correct and validated following the DL consensus mechanism.

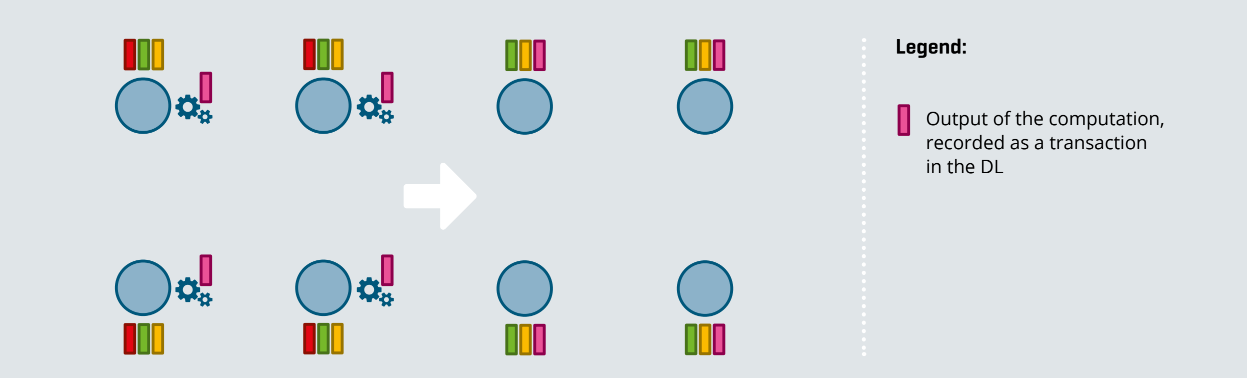

Legend:
Output of the computation, recorded as a transaction in the DL

Figure 5: Output of collective local computations recorded in the distributed ledger

Thus, the *entire DLT system* is responsible for contract execution, and no party with a stake in the outcome has unacceptable levels of control.

The first system to truly explore the potential of smart contracts is Ethereum. It also introduced a contract programming language that has sufficient flexibility to essentially write arbitrary programs.

Standards for all aspects of smart contracts

As an essential tool for taking DLT beyond cryptocurrencies, smart contracts must be considered in their own right by SDOs. Accordingly, ISO/TC 307 has a working group dedicated to this topic - WG 3 *Smart contracts and their applications*. The Technical Report ISO/TR 23455:2019 *Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*[22], published in October 2019, was the first deliverable output by ISO/TC 307.

An ongoing project trying to reconcile blockchain-supported smart contracts with mainstream contractual practice is the ongoing Technical Specification (TS) on legally binding smart contracts (ISO/TS 23259 *Blockchain and distributed ledger technologies — Legally binding smart contracts*[23]). Finally, security of smart contracts is also the subject of a Technical Report under preparation, ISO/TR 23642 *Blockchain and distributed ledger technologies — Overview of smart contract security good practice and issues*[24].

[22] https://www.iso.org/standard/75624.html?browse=tc

[23] https://www.iso.org/standard/75095.html?browse=tc

[24] https://www.iso.org/standard/81772.html?browse=tc

2

Distributed Ledger Technology Landscape

2. Distributed Ledger Technology Landscape

At the time of writing of this report, there are thousands of altcoins and platforms in existence. While it is impossible to survey them all even on a high level, we have chosen a few to describe, essentially based on their apparent appeal to the market. Also, we will not be going into details on Ethereum, Stellar, or Hyperledger Fabric, as these have been already covered in ILNAS' white paper from 2018 [1], but see Section 2.3 for some brief updates on these.

2.1 Platform overview

Table 2 contains a recap of Blockchain platforms that are either a) major platforms, b) discussed in some detail in this technical report, or c) not already listed in ILNAS' previous white paper on Blockchain and technical standardization [1].

Name	Governance		Decentralization	Consensus	Structure	Purpose		Notes
	Maintenance	Access				Stated Use	Smart contracts	
IOTA[25]	IOTA Foundation	Public, permissionless	Partial	Proof-of-Work + Coordinator decision (see Section 2.2.2)	Directed Acyclic Graph (DAG)	IoT	No	A cryptocurrency for the Internet of Things
Ethereum[26]	Ethereum Foundation	Public, permissionless	Total	Proof-of-Work, soon to be Proof-of-Stake	Blockchain	General	Yes	Turing-complete[27] programming language
Bitcoin[28]	Bitcoin.org	Public, permissionless	Total	Proof-of-Work	Blockchain	e-cash	No	The first, and as of June 2021, arguably the most successful, distributed ledger
Steem[29]	Steemit Inc.	Public, permissionless	Partial	Proof-of-stake	Blockchain	Content creation	No	A blockchain solely used to reward creators of content on the social media site Steemit
Ripple[30]	Ripple Labs	Public, permissioned	Partial	Ripple consensus protocol (similar to BFT)	Custom	Payment system	No	It has a system-native currency (denoted XRP), but ultimately payments are made in any fiat currency

Table 1: Some existing blockchain platforms (part 1)

[25] https://www.iota.org/ (accessed 22/03/2021)

[26] https://ethereum.org/en/ (accessed 22/03/2021)

[27] Roughly speaking, a Turing-complete language is one that is rich enough to program any computation. We refer to https://en.wikipedia.org/wiki/Turing_completeness for more formal definitions and additional references.

[28] https://bitcoin.org/en/ (accessed 22/03/2021)

[29] https://steem.com/ (accessed 22/03/2021)

[30] https://ripple.com/ (accessed 22/03/2021)

Sovrin[31]	Sovrin Foundation	Public, permissioned	Partial	BFT (Hyperledger Indy)	Custom	Self-sovereign identity	No	A DL for decentralized digital identity, credential creation, and management
Cardano[32]	IOHK (Input Output Hong Kong)	Public, permissionless	Total	Proof-of-stake (Ouroboros)	Blockchain	General	Yes	Still under development
R3 Corda[33]	R3	Private, Permissioned	Partial	BFT, Raft (see also Section 2.2.1)	Hybrid	General	Yes	Kotlin, Java programming languages, Turing complete
Hyperledger[34]	Linux Foundation	Private, permissioned (but may depend on the underlying framework used)	Partial	Varies with used framework	Varies with used framework	Varies with used framework	Yes	Hyperledger has many different frameworks to choose from, depending on desired applications. “Fabric” and “Sawtooth” are the most commonly used

Table 1: Some existing blockchain platforms (part 2)

[31] https://sovrin.org/ (accessed 22/03/2021)

[32] https://cardano.org/ (accessed 22/03/2021)

[33] https://www.r3.com/corda-platform/ (accessed 22/03/2021)

[34] https://www.hyperledger.org/ (accessed 22/03/2021)

2.2. Platform examples

2.2.1. R3 Corda: An enterprise-grade computing platform

A financial-sector DL consortium

The R3 consortium was founded in 2015, with initially 42 members stemming mostly from the banking community[35]. R3 has since evolved into an enterprise software firm, that works with over 300 stakeholders from the financial industry, including regulators and banks.

R3 set out to create an enterprise-grade DL software that was specifically tailored to the industry of the consortium. This DLT is known as Corda. In [21], the creators of Corda write *"A possible end-state is one in which we have moved from authoritative systems-of-record maintained within firms, and which must then be expensively reconciled, to global authoritative systems-of-record shared between all economic actors: optimization at the level of markets, not at the level of firms"*. Thus, the platform is built for cross-enterprise contracting, primarily in the financial sector.

Corda is open-source software. A Corda-sustained blockchain is a permissioned system, with no underlying cryptocurrency. However, Corda supports smart contracts, called *CorDapps*, written in Java or Kotlin, and can accommodate any relational database management system for the underlying contract data. There is a strong will from the developers to focus on interoperability and integration with legacy systems. There is also a strong will to focus on confidentiality of transacting, especially important in the enterprise setting. For this last point, a specific architectural choice was made.

An architecture that separates transaction validity and transaction uniqueness

Contrarily to many Blockchain platforms like Ethereum, a Corda network does not use global broadcast of participants' transactions to have them committed to an overall ledger. Rather, all transactions are point-to-point, in an effort to maintain the access of contract and transaction data *only* to those parties that are concerned by them. This can be considered to be a "transaction layer" for the system.

However, the ordering and timestamping of transactions, and resolution of conflicts are done by special *notary pools*. In particular, these notaries prevent the recording of invalid transactions (that is, transactions spending already spent output). So, the ledger layer is dedicated to transaction uniqueness, while there is a separate transaction validity layer run solely by the concerned contract stakeholders, see Figure 6 (in contrast to Figure 7). Parties that receive a transaction and activate the contract on that transaction's input check the result themselves, check all signatures, and check the validity of other transactions to which the one at hand makes a reference. The reconciliation of having digital contracts shared only between concerned parties with having a global system for tracking and validation is possible through cryptographic hashing.

Corda provides different options for consensus mechanisms, all based on fault tolerance in order to achieve scalability in transaction speed and throughput. These can be BFT, Raft [22] or others, depending on how much trust the nodes within the notary pool are assumed to place in one another. One may even simply reduce the notary pool to a single node deciding on everything.

[35] https://www.r3.com/history/ (accessed 08/04/2021)

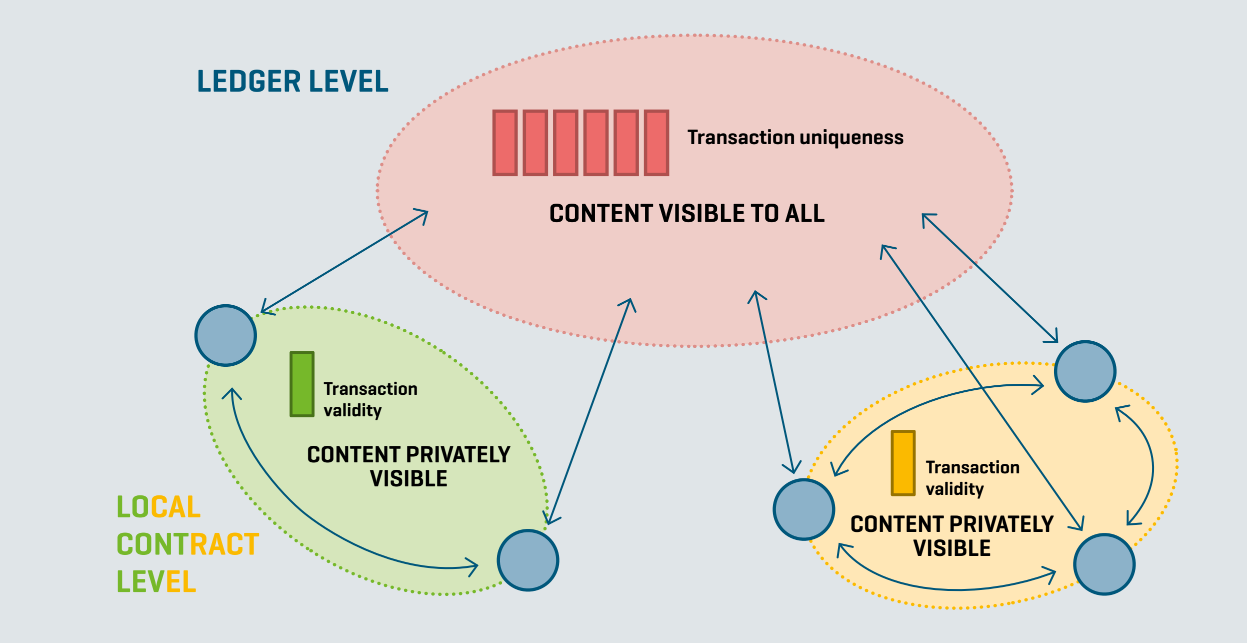


Figure 6: Separate transaction validity and transaction uniqueness layers in Corda

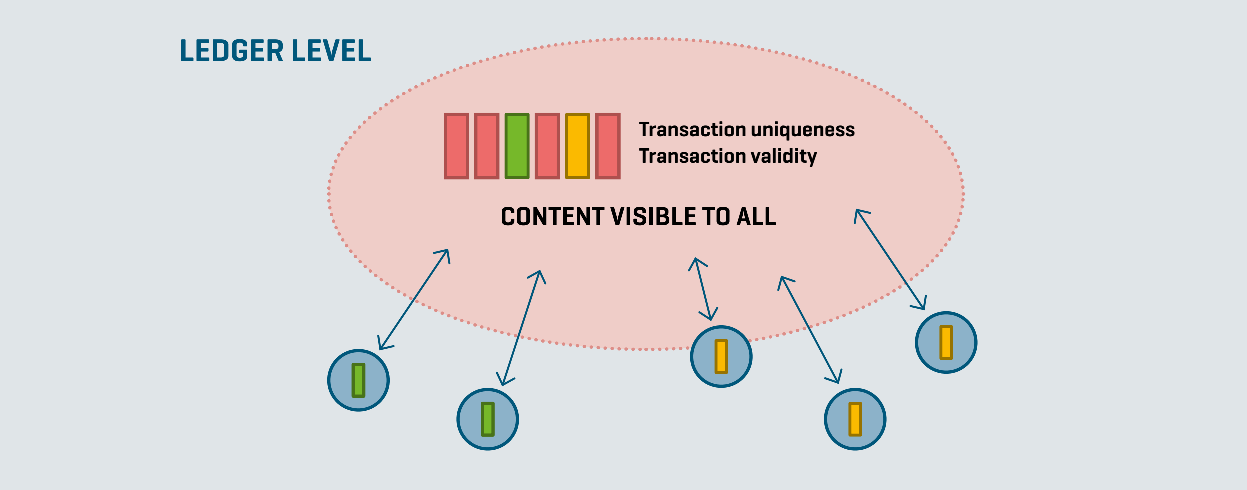


Figure 7: Transaction validity and uniqueness on the same ledger layer, as in e.g. Ethereum

Towards legacy adoption and legal bindings

Corda uses a more restrictive version of the Java Virtual Machine for contract execution. The choice of Java is motivated by the advantages of re-using existing, widespread knowledge in the developer community, in particular to foster adoption. The virtual machine is more restrictive in order to better ensure that consensus is reached in contract execution. The possible programming languages used (Java and Kotlin) are also Turing-complete, for maximized functionality and flexibility.

Corda requires that an entity's legal name be associated with *at most* a single public key, bound to that name using an X.509 certificate. This supports non-repudiation, which is essential for legal bindings. The Corda network governing body will be the one to oversee the process of identity verification and in-network issuance. However, the responsibility of each actor in the network to vet for a party to be allowed to join their local business network rests with that party.

2.2.2. IOTA: A use-case-specific platform

IOTA [23] was designed - and the IOTA Foundation was founded - in Germany, making it an example of a European-based cryptocurrency. The cryptocurrency was launched through an *Initial Coin Offering* (ICO), in November and December 2015[36]. The Foundation was created as a non-profit organization in 2017 by David Sønstebø and Dominik Schiener, two of the four main creators of the technology. IOTA is a public, permissionless DL, and was 26th in market capitalization at the time of writing[37].

Purpose and principles

A cryptocurrency for the IoT…

The creators of IOTA have the vision that their ledger should one day become the DL for the *Internet of Things* (IoT), allowing many, possibly low-powered, simple networked devices to form a data marketplace of their own, enabled namely by seamless *Machine-to-Machine* (M2M) micropayments.

Prerequisites for such micropayments include first the complete elimination of transaction fees and secondly a massive increase in scalability. For the former, it is clear that if a data point costs less than making the payment to access that point's value, then the system is of no use. For the latter, the system needs to mainly scale across two dimensions: the number of system users at any given time and the speed and latency of transactions. Indeed, M2M payments in the future may involve *billions* of devices[38], requiring *simultaneous access* to the payment system, and consumption of data points will necessarily be real-time, forcing the payment system to be so as well. Payment or network lag are unacceptable in this case.

…but not a blockchain

IOTA is an example of a DL that does not have a blockchain-structured transaction history. Instead, successive transactions form a *Directed Acyclic Graph* (DAG) called the "IOTA Tangle".

IOTA's technical strategy to solve the scaling and transaction fee problems is to merge users and miners together, that is, if one wishes to submit a transaction, one *shall* participate in the mining by *actively vetting* at least two past transactions. In theory, this eliminates transaction fees, since there is no longer a need to additionally incentivize validation, as it is fully integrated into transacting in the first place. Also in theory, scalability is at least partially

[36] https://icodrops.com/iota/ (accessed 08/04/2021)

[37] https://coinmarketcap.com/ (accessed 08/04/2021)

[38] https://sustainability.superioressexcommunications.com/iot-market-growth-shows-no-sign-of-slowing/ (accessed 08/04/2021)

solved in that validating capacity increases with the number of users. In other words, the system should improve in speed as it grows in uptake.

Which transactions to validate in order to submit one is up to the submitting node; there are various strategies that can be followed depending on system parameters[39]. Note however that overall this is how the Tangle naturally organizes itself as a DAG: the graph vertices are the transactions, and a directed edge between two vertices indicates that one of the transactions has validated the other, see Figure 8[40].

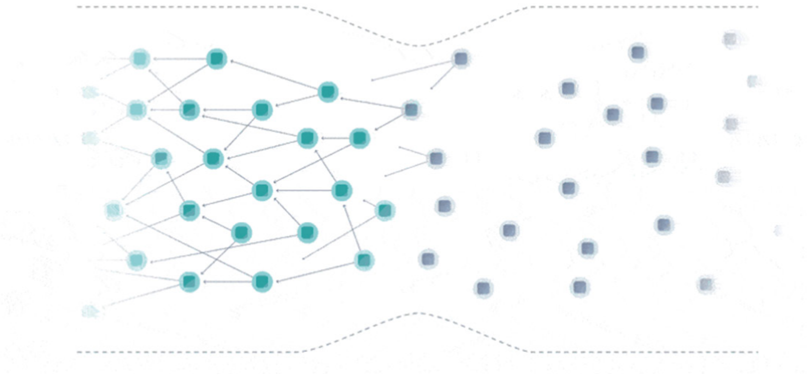


Figure 8: The Tangle's directed acyclic graph structure. The newer transactions are on the right, in dark grey, awaiting validation. Those on the left, in green, are validated.

Some additional safeguards are in place to keep nodes from e.g. flooding the system with too many transactions. For instance, nodes have to solve a small proof-of-work puzzle in order to issue a transaction[41].

Practical challenges

The Coordinator

IOTA's security depends still on most of the participating power being honest, but for this to occur, it needs to reach a critical mass of adoption. Until this happens, the system may be insecure, and this has forced the IOTA Foundation to introduce to the system what is hoped to be a temporary special node called the *Coordinator*. The Coordinator's role is to ultimately validate all transactions even after they have been validated by normal users. This creates a bottleneck that harms scalability, limiting the system for now.

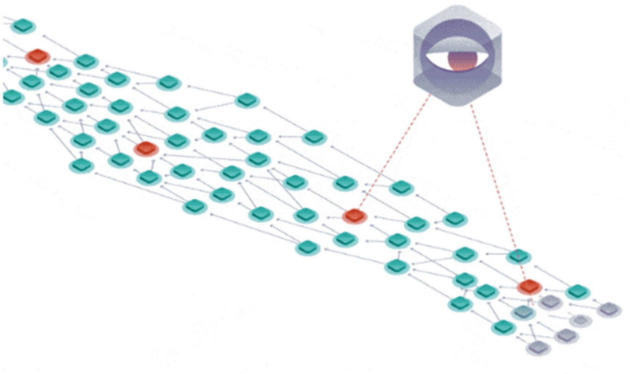


Figure 9: The Coordinator validating transactions[42]

[39] This is part of the research program of the IOTA Foundation, see [71].

[40] Image taken from https://coordicide.iota.org/scalability.

[41] This actually takes proof-of-work back to its very first uses as a spam-control mechanism, see [70].

[42] Image taken from https://coordicide.iota.org/scalability.

The very presence of the Coordinator also has a major side effect on governance of the overall system: since the node is controlled essentially by the IOTA Foundation, IOTA as a whole is unfortunately pulled back towards centralization.

Intense research led by the IOTA Foundation is ongoing to eliminate the Coordinator, an event dubbed the *Coordicide*, see [24].

2.3. Updates on Hyperledger, Ethereum, and Stellar

In this section, we briefly report on the three DL technologies that we placed in the spotlight in the ILNAS white paper from June 2018 [1].

2.3.1. Hyperledger

Hyperledger remains one of the top technologies for permissioned (typically, enterprise-grade) ledgers, and is one of the most active. Indeed, Forbes' February 2021 list of 50 large companies dabbling in Blockchain [25] shows that 26 out of those 50 are using Hyperledger technology. The Linux Foundation-managed umbrella of DL technologies has added, since September 2017 (date of reporting on the technology indicated in Section 2.2 of [1]), at least one DL framework and several tools to its portfolio, listed in Table 2. Furthermore, Fabric 2.0 was released in January 2020[43], adding new tools for the governance of smart contracts and new privacy mechanisms.

Name	Type of component	Short description	Current stage	Start date of current stage
Quilt	Library	An implementation of the payment-enabling Interledger[44] protocol	Incubation	10-2017[45]
Caliper	Tool	A ledger performance-measuring tool, adapted to any of the Hyperledger frameworks	Incubation	03-2018[46]
Grid	Domain-specific	A pre-built combination of Hyperledger projects into a DL solution for supply-chains	Incubation	12-2018[47]
Transact	Library	A library for writing ledger-agnostic smart contracts	Incubation	05-2019 [48]
Aries	Library	A library for Blockchain-based digital credentials and identity	Incubation	05-2019[49]
BESU	Framework	A Java-based Ethereum client. The first Hyperledger framework that can run on a public blockchain	Active	08-2019[50]

Table 2: Hyperledger projects that have appeared since September 2017 (part 1)

[43] https://www.hyperledger.org/announcements/2020/01/30/hyperledger-announces-hyperledger-fabric-2-0 (accessed 08/04/2021)

[44] https://interledger.org/ (accessed 08/04/2021)

[45] https://www.hyperledger.org/blog/2017/10/16/hyperledger-gets-cozy-with-quilt (accessed 08/04/2021)

[46] https://www.hyperledger.org/blog/2018/03/19/measuring-blockchain-performance-with-hyperledger-caliper (accessed 08/04/2021)

[47] https://www.hyperledger.org/projects/grid (accessed 08/04/2021)

[48] https://wiki.hyperledger.org/display/transact (accessed 08/04/2021)

[49] https://www.hyperledger.org/blog/2019/05/14/announcing-hyperledger-aries-infrastructure-supporting-interoperable-identity-solutions (accessed 08/04/2021)

[50] https://www.hyperledger.org/blog/2019/08/29/announcing-hyperledger-besu (accessed 08/04/2021)

Avalon	Tool	A tool to securely move on-chain operations to a trusted computing environment off-chain	Incubation	10-2019[51]
Ursa	Library	A unified cryptographic library for use in other Hyperledger projects	Incubation	11-2019[52]
Cactus	Tool	A tool to allow interoperability across several blockchains including Fabric, BESU, Quorum and Corda	Incubation	05-2020[53]

Table 2: Hyperledger projects that have appeared since September 2017 (part 2)

2.3.2. Ethereum

As of January 2021, Ethereum remained, behind Bitcoin, the second most valued DL in terms of market capitalization, at over $119Bn[54].

Ethereum is still undergoing its transformation to reach "2.0". The main target features of this release – which will be a managed hard fork – will be the *replacement of Proof-of-Work by Proof-of-Stake* to reach consensus, and the use of *sharding* (sharding for Ethereum is explained in Figure 10). These are expected to greatly increase the scalability of the platform, which is its greatest weakness, to one of the Ethereum co-creators' own admission[55]. Major Ethereum updates are hard forks, which means that a local software update is *mandatory* in order for a node's participation to continue. The following list summarizes these events so far:

- **Frontier.** Started July 2015. The public beta launch of Ethereum. As such, not really a fork.
- **Homestead.** Started March 2016. Launch of the first "production-ready" version of Ethereum.
- **DAO fork.** Started July 2016. An initially unplanned hard fork to reverse the effects of the DAO hack. Led to the creation of Ethereum Classic.
- **Byzantium.** Started October 2017. Brought improvements to security and streamlined the protocol.
- **Constantinople.** Started January 2019. Technical changes include optimization of execution of larger-code contracts and the reduction of block mining rewards. Along with Byzantium, these two phases are to prepare the transition from proof-of-work to proof-of-stake.
- **Istanbul.** Started December 2019. Technical changes to better accommodate on-chain privacy technologies and expand function possibilities for smart contracts.
- **Deployment of staking contract.** Started October 2020. Created the ability to stake value in Ethereum through a contract, a necessary step towards implementing proof-of-stake.
- **Beacon chain launch.** Started December 2020. **This is the phase Ethereum is currently in**. This is not a fork; rather it is the launch of a new chain meant to support sharding result reconciliation.

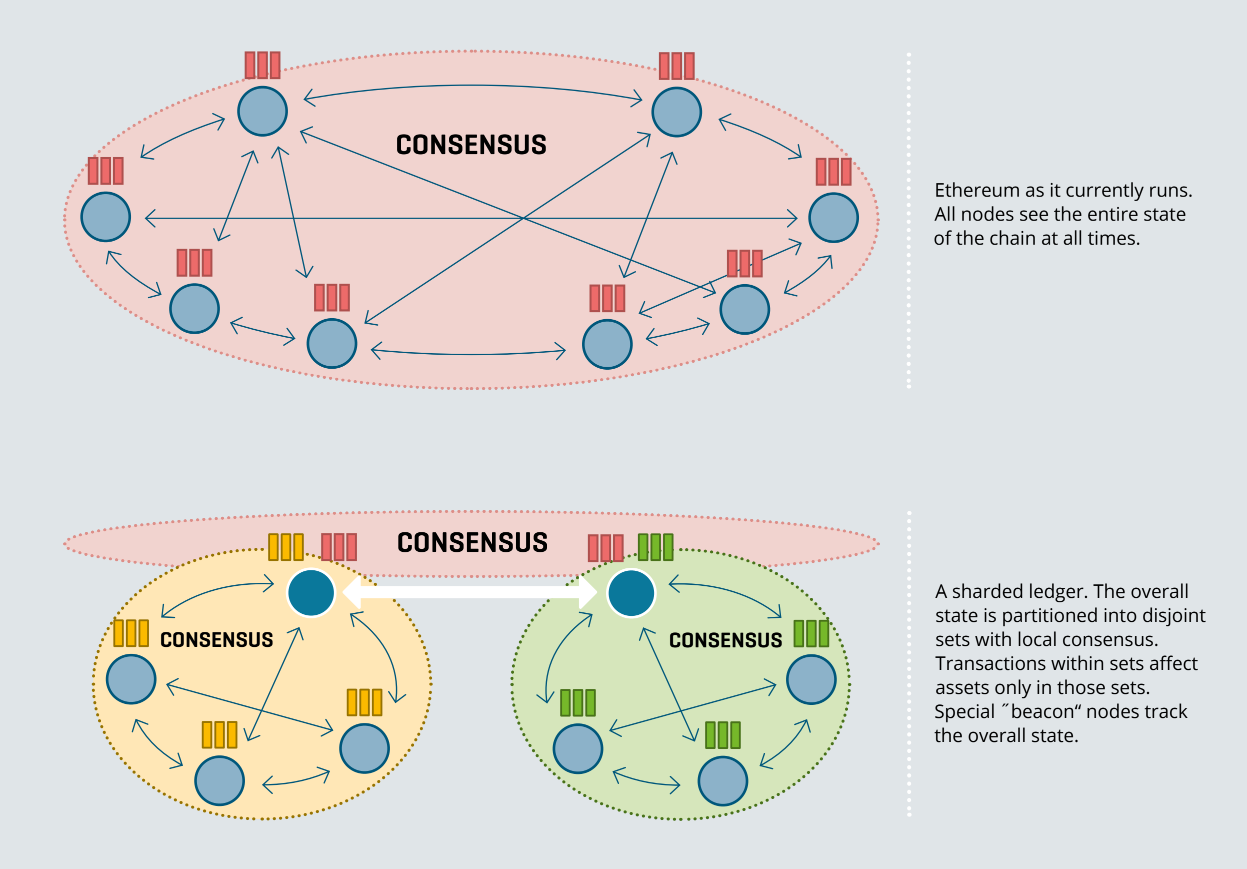
[51] https://www.hyperledger.org/blog/2019/10/03/introducing-hyperledger-avalon (accessed 08/04/2021)

[52] https://wiki.hyperledger.org/display/ursa (accessed 08/04/2021)

[53] https://www.hyperledger.org/blog/2020/05/13/tsc-approves-hyperledger-cactus-as-new-project (accessed 08/04/2021)

[54] https://coinmarketcap.com/ (accessed 05/01/2021)

[55] https://cointelegraph.com/news/vitalik-buterin-talks-scalability-ethereum-blockchain-is-almost-full (accessed 05/01/2021



Ethereum as it currently runs. All nodes see the entire state of the chain at all times.

A sharded ledger. The overall state is partitioned into disjoint sets with local consensus. Transactions within sets affect assets only in those sets. Special ˝beacon“ nodes track the overall state.

Figure 10: Sharding in Ethereum

2.3.3. Stellar

Stellar has gained considerable traction in the last years. In April 2021, it supported 71 projects in total, providing wallets (Solar Wallet), analytics (Stellar Expert), tokenization (MINTX), and more. The Stellar network has roughly 130 active nodes, per stellarbeat.io[56], and in 2019 the number of Stellar accounts has risen from 2,4M to more than 4,3M. Its market capitalization has also significantly increased, from $3,6Bn in June 2018 to over $11Bn in April 2021.

[56] https://stellarbeat.io/ (accessed 08/04/2021)

2.4. Blockchain and Smart ICT

In the context of Luxembourg's focus on the ICT sector for standardization[57], four major technologies – including Blockchain – have been singled out for their potential, the three other being Artificial Intelligence (AI), the Internet of Things (IoT), and Cloud Computing. We give some insight here on how these three other technologies interact, or may interact in the future, with Blockchain and DLT.

IoT, AI and Cloud Computing all have a major element in common: a heavy reliance on data. It is therefore no surprise that Blockchain is mostly considered as a means to enhance data security, traceability, and availability. Since the application of Blockchain to Cloud Computing and the IoT were already covered in the ILNAS 2018 white paper [1] the reader can find additional references of interest there.

2.4.1. Blockchains and Artificial Intelligence

There is no real set definition of Artificial Intelligence; a good discussion and history on this can be found in the ILNAS AI white paper [26]. For the purpose of this report we can oversimplify, and think of AI as a combination of computer hardware and software that emulates humans' thinking abilities.

One of the most researched AI types is *machine learning*, which requires huge volumes of high quality *training data* to fine-tune adequately. Often, the creation, ownership and management of such datasets are possible solely by global-scale companies that have the necessary collecting capabilities. This makes machine learning difficult to access by a more general market, thereby stifling innovation and opportunity for all other stakeholders. Centrally-managed pools of data are also more amenable to manipulation, especially from insider attacks [28].

Blockchains can aid in tracing data from its origin, thereby being able to evaluate its quality. The key Blockchain characteristic used here is the database's near-immutability. The ledger is close-to-impossible to tamper with, thus data can be vetted, e.g. based on its origin and history.

Blockchains can also serve as a support platform for collectively created and managed datasets, around which business models for all may be imagined. This is sometimes designated "data democratization" [29].

Besides new data governance schemes, Blockchain technology is also envisaged to aid in providing otherwise prohibitively expensive, already-trained machine learning models to companies having a real need for AI, but lacking the resources to implement it end-to-end in house [30]. Blockchain thus becomes an enabler for AI-as-a-Service.

Since both AI and Blockchain are fields in their infancy, their full convergence likely is still far off. It is imagined by some that one of the forms it could take is that of fully decentralized AI, wherein multiple human-independent autonomous agents will communicate, transact, and learn from each other to bring enhanced services to society with minimal human intervention [29]. It is also the subject of ongoing work in the standards developing organization ITU-T, where the project *Overview of convergence of artificial intelligence and blockchain*[58] is under development. In the meantime, research is pointing to more mid-term uses in domains as diverse as financial compliance [31], cyber security for energy grids [32], and even pandemic management [33] (see also Section 3.4).

[57] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-luxembourgeoise-2020-2030.html

[58] https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14651

2.4.2. Blockchains and the IoT

The Internet of Things can loosely be defined as the paradigm wherein typically inanimate or "dumb" objects are endowed with some form of data connection to other objects – typically through the Internet – in order to share data and/or act on their environment. Thus, these objects become "smart". More information on efforts to define the IoT and the challenges inherent to its large scale implementation can be found in ILNAS' IoT white paper [27] and the follow-up National Technical Standardization Report from 2020 [34].

The main vision regarding Blockchain and IoT described in [1] is still valid today: to allow connected "things" to interact - and even inter-transact - in an architecture that no longer relies on single, cloud-based data silos and data flows. Indeed, it has already been recognized that direct connections between devices is essential to allow efficient scaling of networks that could potentially contain billions of devices [35]. For instance, smart contracts can be used on a Blockchain platform (organized as a peer-to-peer network infrastructure between IoT objects) to automatically instruct a connected device to make a payment to some other device (or to instruct another connected device to act on its environment, or some other action) based on real-time sensor data satisfying certain conditions specified by the contract. One can imagine an autonomous car being directed to an available parking spot by a parking drone, and rewarding that drone with a micro-payment upon being actually parked.

Other use cases that apply blockchains to the IoT setting include, for instance:

- Blockchain-based access control to IoT devices [36] [37],
- Support to 5G IoT deployment [38], and
- Blockchain architectures for healthcare-oriented IoT platforms [39].

Note that several SDOs are also examining this point, for instance ISO and IEC's technical subcommittee ISO/IEC JTC 1/SC 41 *Internet of Things and Digital Twin* and ITU-T's Study Group SG 20 *IoT*, *Smart Cities and Communities*, see Sections 4.2.2 and 4.5.2.

2.4.3. Blockchains and Cloud Computing

Cloud computing is, almost by definition, somewhat a contrasting technology to Blockchain. Indeed, the most defining element of Cloud Computing is its pooling of resources in order to yield compute infrastructure, software platform power, and even applications as utilities. This is a virtual centralization of power. In addition, it can be argued that worldwide, the Cloud computing market is dominated essentially by "centralized giants" such as Google, Amazon, Microsoft and Alibaba. While access to pools of computing power can be readily applied to blockchain mining activity, other ways Blockchain interacts with the Cloud are less obvious.

Lately, data protection and control have garnered considerable attention. This is all the more true now that Cloud storage is placing massive amounts of data in the hands of third parties. Accordingly, a lot of research has been put into leveraging blockchains to increase the assurance of data provenance in the cloud, e.g. [40], [41], and [42].

Another recent trend in Cloud computing to help circumvent the monopoly of solutions is the use of cloud exchanges. A cloud exchange is a service that creates one or more connections for a single user to possibly different cloud services depending on that user's needs. A cloud exchange can offer for instance to match a user's requirements with different combinations of cloud services, help in providing appropriate service level agreements, and even integrate a reputation mechanism for cloud service providers. In [43], the authors show how using Blockchain technology, cloud exchanges themselves can become distributed entities, in order to avoid them becoming single points of failure.

2.5. Technical challenges

A good way to view the main challenges posed to all of these platforms is Vitalik Buterin[59]'s description of the "Blockchain trilemma"[60]. In a nutshell, it is the statement that in the design of a blockchain, privileging one of scalability, security, and decentralization necessarily comes at the expense of the other two, see Figure 11. For instance, Bitcoin suffers from transaction throughput and transaction speed scalability (although it supports millions of wallets); but, it is a highly decentralized platform, and is arguably the most secure with regards to its consensus achieving and immutability.

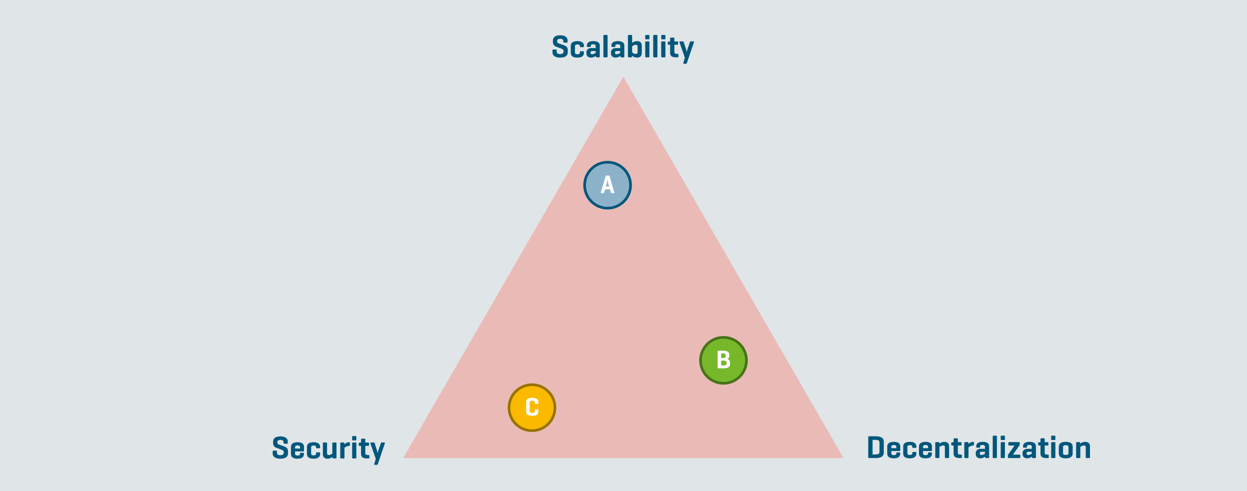


Figure 11: The distributed ledger trilemma. Blockchain designs A, B and C cannot enjoy all three ideal properties fully and simultaneously

IOTA can be viewed as another example. Indeed, the DAG-based architecture in theory allows for scalability in both number of accounts and transaction speed and throughput, even strongly correlating the two. On the other hand, IOTA, as we have seen in Section 2.2.2, has been forced to make use of a centrally-controlled Coordinator node to keep the system secure, and there is no assurance so far that this can be easily removed. As for permissioned solutions such as Corda, clearly decentralization is heavily limited in favor of scaling in speed and security.

Some efforts have been made to take Blockchain scaling to another layer; these are so-called "layer-2" solutions, built over a "layer-1" blockchain. A good example of this strategy is the Lightning Network [44]. The idea behind this network is to construct special fund-locking smart contracts between two parties with accounts on a "slow" blockchain (the solution was initially developed for Bitcoin). Creating such a contract requires a Blockchain transaction, as does closing the contract. However, the contract *balance* between the parties can be adjusted between contract creation and closure simply by creating and sending – but not recording on-chain – real Blockchain transactions off-chain. Only when a final balance is reached does one of the parties actually record the transaction on-chain, thus closing the contract. This creates *micropayment channels* and more generally a *micropayment network*. See [45] for more details. The Lightning Network is still rather nascent technology, with its own set of challenges (linked to the locking of funds, the difficulty of routing payments, and other issues), but it has seen some uptake, see [46].

[59] Co-inventor of Ethereum

[60] https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/sharding/

Usability remains a problem for DLs, and as is the case with most IT systems, usability finds itself clashing with security, particularly in the area of authentication. The seminal paper "Why Johnny can't encrypt" [47] demonstrated the difficulty that ordinary users have in managing the use of public and private keys, and the problem is still present to this day. So, it is no surprise that this causes a major "security vs. usability" problem in DLT, where the use of public/private key pairs from cryptography is absolutely critical. Indeed, the loss of a private key in Ethereum for instance means the loss of all of the funds supported by it. There are different ways to hold one's private keys, each with their own set of problems:

- Keys can be kept in *hard wallets*, that is hardware tokens in the user's custody. These are the most secure, but are amenable to theft and loss. It places considerable cognitive burden on the user;
- Keys can be kept in *soft wallets*, that is in software storage:
    - The software can be the user's PC or mobile device, increasing seamless interaction with the blockchain, but also increasing the threat of theft by malware or spyware;
    - The software can be hosted on a service provider's server, typically that of a cryptocurrency exchange. This also increases seamless interaction with the blockchain through the provider, but it places the private key in a trusted third party's custody, and this party is not immune to major hacks[61].

[61] For example, the Mt. Gox hack, see https://blockonomi.com/mt-gox-hack/ (accessed 08/04/2021).

3

Initiatives and applications

3. Initiatives and applications

3.1. European Union initiatives

The European Union has taken a keen interest in Blockchain technologies, in support of the development of the Digital Single Market. Most notably, the European Blockchain Partnership[62] was signed in April 2018 in order to organize a coherent, pan-European strategy for the development of the technology. As of February 2021, 26 EU Member States (and two additional European countries), including Luxembourg, were signatories.

Notable projects in this context at the EU level include the EU Blockchain Observatory and Forum and the European Blockchain Services Infrastructure (EBSI).

3.1.1. The European Blockchain Observatory and Forum

The European Blockchain Observatory and Forum [48] was launched by the European Commission (EC) in February 2018. It is led by the EC's Directorate-General of Communications Networks, Content and Technology (DG CNECT)[63]. The forum aims to essentially be a general knowledge resource on the ever-changing European Blockchain landscape. Tasks undertaken to accomplish its missions include:

- mapping and documenting Blockchain initiatives across the continent,
- advising the EU on how to further encourage development,
- providing research papers[64] and reporting[65] on trends,
- organizing thematic workshops and other events[66], and
- providing notable news.

3.1.2. The European Blockchain Services Infrastructure

The European Blockchain Services Infrastructure (EBSI)[67] has been under development since 2019, as one of the Connecting Europe Facility's Building Blocks[68]. It is a network of European nodes spread out across the continent as an infrastructure to Blockchain-supported cross-border public services. One can see it as a continent-wide, inter-governmental use case, with a strategic vision spanning sustainability, citizen and enterprise mobility, and regulatory compliance.

The broad objective of the EBSI is to streamline cross-border public services for European citizens, in full compliance with EU legislation, such as the General Data Protection Regulation (GDPR)[69] and eIDAS[70]. The use of Blockchain technologies will allow such services to be more transparent, trustworthy, and most notably completely cross-border.

[62] https://ec.europa.eu/digital-single-market/en/european-blockchain-partnership-0 (accessed 31/03/2021)

[63] https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en (accessed 31/03/2021)

[64] https://www.eublockchainforum.eu/knowledge (accessed 31/03/2021)

[65] https://www.eublockchainforum.eu/reports (accessed 31/03/2021)

[66] https://www.eublockchainforum.eu/events (accessed 31/03/2021)

[67] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI (accessed 31/03/2021)

[68] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home (accessed 31/03/2021)

[69] https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 31/03/2021)

[70] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed 31/03/2021)

Four projected sub-use-cases are planned as of early 2021:

- notarization,
- electronic diplomas,
- self-sovereign identity, and
- secure and trustworthy data sharing.

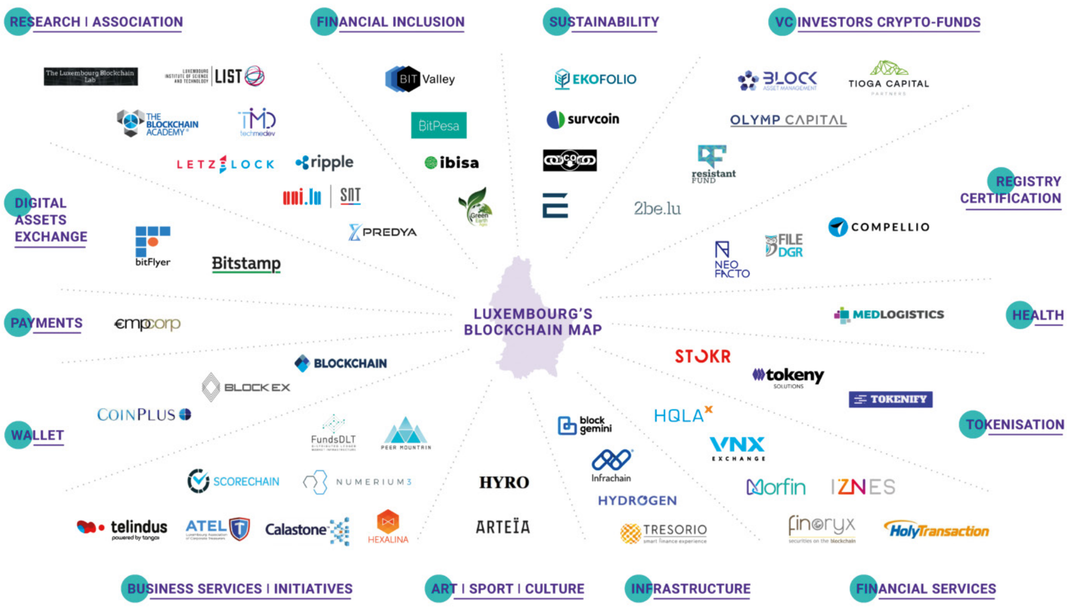
The chain itself is a “public-permissioned” blockchain, with validating nodes being managed by the EC and Member States. The architecture is based on 8 principles: Security, Interoperability, Scalability, Performance, Auditability, Integrity, Privacy, and the use of an Open approach. Among its technical requirements one finds the support of distributed applications, on-and-off-chain storage capabilities (depending on data criticality) and interoperability with existing and future systems.[71]

As of February 2021, the network was composed of 25 live nodes, with 11 nodes under development (however the exact list of nodes was not at the time publicly available).

[71] The image is taken from https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI#cef-ebsi-get-started, accessed 15/04/2021.

3.2. National scene

There is a quite vibrant Blockchain community in Luxembourg, composed of all sorts of actors, including start-ups, research centers, and associations, see Figure 12 (non-exhaustive list, compiled and place into a figure by the Luxembourg House of Financial Technology[72]). Note also that the domains covered are also quite varied: wallet providers, exchanges, tokenization services, and even the provisioning of infrastructure are proposed.



Compiled with the support of ALFI and the Luxembourg Blockchain Lab

© The LHoFT Foundation

Figure 12: A snapshot of the Luxembourg Blockchain scene[73]

Blockchain is viewed by the government of Luxembourg as a promising technology. The Grand Duchy aims to become a "pioneer in the Blockchain world"[74]. In support of this, Luxembourg has also been, since 2019, updating its legislation in the financial sector in order to better accommodate Blockchain and DLT. For instance, the law passed in 2019 gives additional legal recognition to securities held and transferred via these technologies[75]. This law was further extended in January 2021[76] through a new law which enables direct issuance of securities over blockchains.

[72] https://lhoft.com/en/ (accessed 31/03/2021)

[73] Image from the LHoFT's Luxembourg Blockchain map, found at https://lhoft.com/en/insights/the-luxembourg-blockchain-map/, (accessed 25/05/2021)

[74] https://luxembourg.public.lu/en/invest/innovation/blockchain.html (accessed 31/03/2021)

[75] http://legilux.public.lu/eli/etat/leg/loi/2019/03/01/a111/jo

[76] http://legilux.public.lu/eli/etat/leg/loi/2021/01/22/a43/jo

3.3. Applications snapshot

The first and most notorious application of DLTs is the implementation of decentralized electronic cash. Bitcoin [2] was the first such implementation, using proof-of-work consensus, and it remains the leader in estimated market capitalization and uptake [49]. Most implemented DLTs support, among other features, a native "coin" with which to make on-chain monetary transactions, e.g. Ethereum has Ether. In total, there are just under 4 500 different cryptocurrencies, although not all carry the same value.

In Section 3.6, we will describe the use of DLTs to define special kinds of cryptocurrencies that attempt to maintain stability, typically by directly pegging their units of value to those of some "real" resource. These are called *stablecoins*; the Diem project [50] (formerly known as the Libra project) is perhaps the most well-known example.

These are far from the only applications that DLTs have. Table 3 gives a non-exhaustive list of sectors in which DLTs can make, or are already making in some cases, their impact felt.

Sector	Domain	Companies/organizations involved	Purpose
Financial sector	Cryptocurrencies	Bitcoin[77]	P2P, decentralized electronic cash system
	Payments	JP Morgan-Chase[78]	Fast clearing of payments between transactors
	Wallet provisioning	Coinplus (Luxembourg)[79]	Hardware crypto-currency wallet provider
Tracking goods	Shipping	TradeLens[80]	Tracking shipping goods
	Art	Verisart[81]	Tracking artwork
	Food	Carrefour[82]	Tracking food provenance
	Land registration	India[83]	Tracking deed ownership
Tracking data	Identity management	Sovrin[84]	Electronic identity, decentralized Public-key infrastructure
Government and governance	General public services	European Blockchain Services Infrastructure[85]	Notarization, tracking diplomas, European self-sovereign identity, data sharing
	General public services	Ministry for Digitalisation (Luxembourg)[86]	Public administration services
Energy	Peer-to-peer energy market	Arizona State University[87]	Enabling a fair and decentralized microgrid
Infrastructure as a service	Blockchain infrastructure	Infrachain (Luxembourg)[88]	Providing permissioned ledger access as a service to smart contract developers

Table 3: DLT use cases by sector. The listed examples range from "proofs-of-concept" to "in production", in no particular order

[77] https://bitcoin.org/en/ (accessed 22/03/2021)

[78] https://www.jpmorgan.com/global/news/digital-coin-payments (accessed 22/03/2021)

[79] https://www.coinplus.com/ (accessed 22/03/2021)

[80] https://www.tradelens.com/ (accessed 22/03/2021)

[81] https://verisart.com/ (accessed 22/03/2021)

[82] https://www.carrefour.com/en/group/food-transition/food-blockchain (accessed 22/03/2021)

[83] https://www.undp.org/content/undp/en/home/blog/2018/Using-blockchain-to-make-land-registry-more-reliable-in-India.html (accessed 22/03/2021)

[84] https://sovrin.org/ (accessed 22/03/2021)

[85] https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI (accessed 22/03/2021)

[86] https://gouvernement.lu/fr/actualites/toutes_actualites/communiques/2019/05-mai/23-hansen-blockchain.html (accessed 15/04/2021)

[87] https://blockchain.asu.edu/p2p-energy-trading/ (accessed 22/03/2021)

[88] https://infrachain.com/ (accessed 22/03/2021)

The European Blockchain Observatory and Forum is a good source for monitoring blockchain projects that exist in Europe [48].

New technology is always accompanied by excessive hype, and for Blockchain and DLT, the situation is no different. This tends to lead to situations where blockchains are forced into use-cases where they serve no actual purpose[89]. The working group WG 6 *Use cases* in ISO/TC 307 is tasked with isolating, studying and reporting on use cases of Blockchain and DLT that show a real added value to disintermediation in certain scenarios. They are preparing a technical report ISO/TR 3242 *Blockchain and distributed ledger technologies – Use cases*[90] on this topic.

3.4. Pandemic prevention and management

The COVID-19 pandemic has had an effect on the world's approach to the use of ICT, so it is fitting to mention how this influences, or is influenced, by Blockchain technologies.

First, the global crisis has exacerbated supply chain efficiency problems, in particular regarding internationally moving goods, see [51] [52]. This was seen for physical goods ranging from medical devices to foodstuffs [53]. Since supply chain efficiency is probably the most popular use case for Blockchain and DLT outside of cryptocurrency, it is no surprise that some solutions supported by it have gained prominence (e.g., see work by VeriTX[91] and Rapid Medical Parts[92], aiming to combine a Blockchain-based parts tracing system with 3D printed manufacturing for medical devices).

The pandemic has also placed in the spotlight the need to make available, in a simultaneously global and near-real-time manner, certain key data points used to synchronize governmental as individual responses, such as infection rates. Crucially, this data needs to be trustworthy and trusted by all actors involved, as hard-to-verify sources inject themselves in official discourse with much greater ease than believed [54]. Other issues that have come to light include the spread – much faster than the virus itself – of disinformation, in particular through social media [55]. Some projects have been launched to take issues such as these on, such as MiPasa[93]. Staying on the topic of data, user privacy is a regularly-cited issue for contact tracing applications [56]; research is in the process of addressing this using Blockchain technology, see e.g. [57].

Certain aspects related to payments and finance are viewed through a new lens as well. The world has been forced into living in a much more digital way, creating an opening for more electronic transactions. A certain distrust of physical currency has also been observed, for fear of spreading the virus through contact with coins and bills. This in theory favors the uptake of cryptocurrency [51]. Other monetary considerations include donation tracking, as there has been a general massive uptake in generosity [58]. Finally, smart contracts can simplify and streamline the processes of acquiring insurance and making claims [58] [59].

In terms of human resources available to actually take on the virus, a real struggle to find and onboard medical professionals has been observed. This is particularly important in the midst of a pandemic. And the issue has the potential to worsen, as wave-after-wave of infections exhaust a frontline stretched to the limit [60]. Streamlining access to professional credentials in a privacy-friendly way is within reach using Blockchain identity management technology [61].

[89] A typical example is thinking a blockchain is necessary when a distributed database would most likely be much more effective, see for instance https://101blockchains.com/blockchain-vs-database-the-difference/ (accessed 22/03/2021) for a nice comparison.

[90] https://www.iso.org/standard/79543.html?browse=tc

[91] https://www.veritx.co/ (accessed 01/04/2021)

[92] http://rapidmedicalparts.com/ (accessed 01/04/2021)

[93] https://mipasa.org/ (accessed 01/04/2021)

3.5. Property management

Land registration is heavily dependent on paper trails, especially for older properties. Property deeds can be stored for decades before ever needing to be used again, and records can end up lost or destroyed. This could also be the case, although to a lesser extent, even if digitized and recorded on a centralized server. However, care must in this latter case still be taken to prevent fraudulent modification, either through hacking or through an insider attack.

Benefits of using a blockchain to trace property ownership include increasing transparency and accessibility to ownership documents, thus simplifying overall property management and preventing fraud (such as double-selling). Immutability properties of a blockchain make it exceedingly difficult to maliciously alter property records (or any other document recorded on the system). It also makes more readily available the ownership history of a particular property. Potentially mutually untrusting stakeholders that can benefit from such a system are buyers and sellers, but also local governments and property brokers[94]. Finally, a reduction in intermediaries and a digitization of the system (beyond simply scanning documents for digital safekeeping) could potentially speed up processes (as it is well-known that the purchase of a property can take weeks, if not months). See Figure 13 and Figure 14 for an example of how a blockchain could integrate itself within a property management architecture in order to improve trust and efficiency.

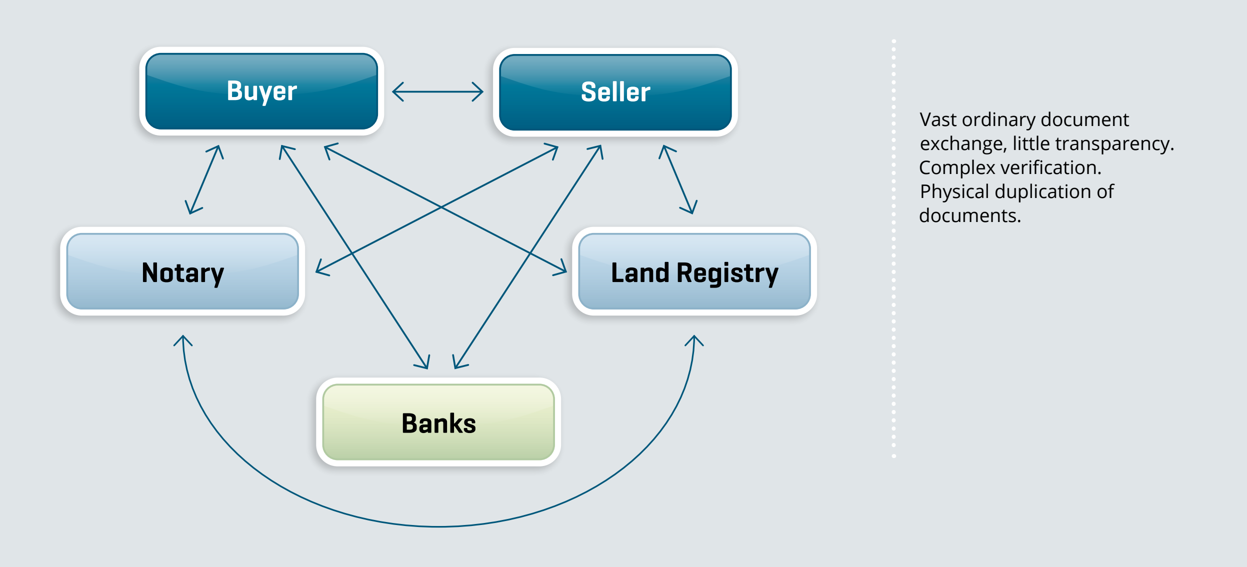

Buyer
Seller
Notary
Land Registry
Banks
Vast ordinary document exchange, little transparency. Complex verification. Physical duplication of documents.

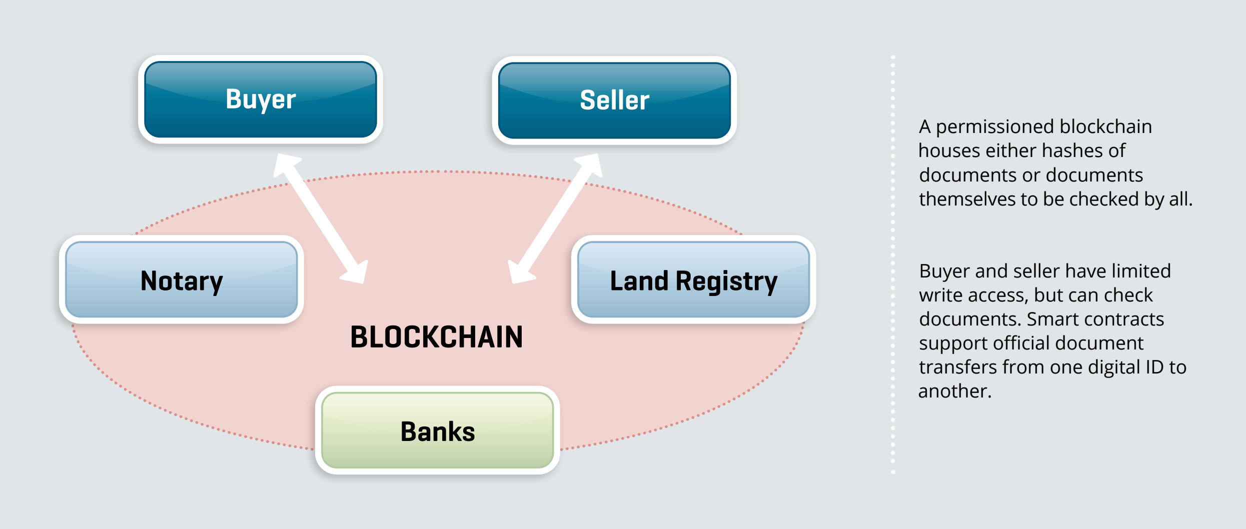
Figure 13: A classical architecture in property transfer

Uptake of Blockchain technology in land registration has for instance happened in the Republic of Georgia[95] [62] and in Sweden[96]. Other areas where this has happened (either in full adoption or as a pilot) include The United Arab Emirates, Illinois's Cook county (in the United States of America), and Ghana [63].

[94] http://cyprusreview.org/index.php/cr/article/view/579/502 (accessed 01/04/2021)

[95] https://www.newamerica.org/digital-impact-governance-initiative/digital-impact-and-governance-initiative-projects/digi-blogs/project-capsule-georgia-land-titling-system/ (accessed 29/03/2021)

[96] http://revolutionofthings.com/sweden-uses-blockchain-for-real-estate-purchases/ (accessed 31/03/2021)



A permissioned blockchain houses either hashes of documents or documents themselves to be checked by all.

Buyer and seller have limited write access, but can check documents. Smart contracts support official document transfers from one digital ID to another.

Figure 14: Blockchain-supported architecture for property transfer

It should be noted that property registration also has considerable points of contact with the legal system, and the complexities inherent to this are not to be underestimated [64]. Blockchains are not likely to replace notaries; nor should one expect to suddenly see entire deeds made available solely on distributed ledgers in the near future. Rather, they will bring more transparency to the overall process. And, it would make more sense to adopt a more sub-services (such as land conveyance or mortgage management) approach at first, rather than expect to change an entire land registry system [65].

3.6. Stablecoins

The imagination of developers, entrepreneurs, and researchers notwithstanding, it remains the case that decentralized cryptocurrency is at the moment the predominant *actually deployed* use case for Blockchain technology. In fact, it is more and more the case that mainstream businesses are accepting them as payments[97].

However, a lingering characteristic – at least for now – of these forms of e-tender remains their instability. Fiat currency is, for the most part, much less volatile than cryptocurrency. Taking Bitcoin as an example, on 24/10/2019 one bitcoin was priced at nearly $7,500, and *just two days later*, at close to $9,600. Then, if one looks at 09/04/2021, one finds that one bitcoin had a value hovering around $58,000, that is almost 6-to-7 times the previously cited values[98] (also see Figure 15).

[97] https://www.businessinsider.com/more-companies-accepting-bitcoin-cryptocurrency-paypal-starbucks-2021-4?r=US&IR=T (accessed 09/04/2021)

[98] Numbers taken from the historical data found at https://coinmarketcap.com/currencies/bitcoin/ (accessed 09/04/2021)

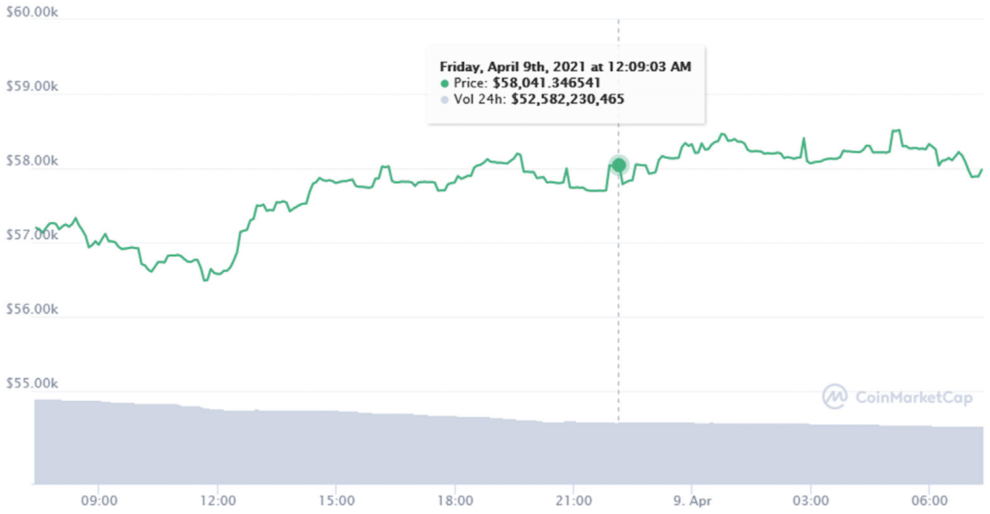


Figure 15: Bitcoin price on 09/04/2021[99]

One can argue that price volatility might diminish as a given cryptocurrency gains in uptake, since this vouches for its long-term sustainability. But in the meantime, a kind of cryptocurrency *designed to be non-volatile* has made its appearance in the crypto-landscape: the Stablecoin.

Stablecoins are cryptocurrencies that declare their unit value as equal to that of a unit of value from a pooled external asset. This process is called *pegging*. The most common, and in some sense easiest, external asset to peg a coin to is a fiat currency, but other commodities are used as well, such as gold. Among the most popular stablecoins are those pegged to the US dollar, such as Tether[100]. Stablecoins pegged to the Euro are not so popular yet, but are making an appearance[101]. There are also stablecoins that are algorithmically stabilized, but these are not as durable, at least not quite yet[102].

Advantages of such coins include being able to speed up settlements and lower transaction fees, especially cross-border[103]. This is due to the underlying cryptocurrency being able to do away with more intermediaries, a feature that could be further enhanced in the future with the development of smart contracts[104].

They do pose certain challenges, however. The first is that the stability of the underlying coin is only as good as that of the asset it is pegged to. When pegged to the US dollar or the Euro, this is reasonable, but not all fiat can make this claim. The second challenge is one of storage and ultimately, degree of centralization and scale. For a stablecoin to gain and keep trust, it must be backed by a pool of assets that correspond to its overall value at all times, e.g. an owner of 1M units of USDT (the unit managed by Tether) should be tradeable to Tether Operations for $1M, as one USDT is defined as equivalent to $1. Thus, those responsible for the coin's upkeep have to be able to back its value. The concerned assets still require to be stored and managed, e.g. by banks or some other means. This makes scaling coin supply non-trivial, and also re-introduces centralization and trust problems. More details on the classifications and challenges of stablecoins can be found for instance in [66] and [67].

[99] From https://coinmarketcap.com/currencies/bitcoin/

[100] https://tether.to/ (accessed 09/04/2021)

[101] https://cointelegraph.com/news/euro-stablecoin-launched-on-stellar-by-one-of-europe-s-oldest-banks (accessed 09/04/2021)

[102] https://cointelegraph.com/news/algorithmic-stablecoins-aren-t-really-stable-but-can-the-concept-redeem-itself (accessed 09/04/2021)

[103] https://medium.com/stably-blog/top-use-cases-and-benefits-of-stablecoins-4f1ceab57d00 (accessed 09/04/2021)

[104] https://www.bitprime.co.nz/blog/stablecoins-types-use-cases-and-benefits/ (accessed 09/04/2021)

Perhaps the most prominent interest in Stablecoins was generated when the Diem association, formerly known as the Libra association, attempted to launch a global stablecoin backed by an overall pool of resources owned by would-be members of the underlying foundation[105]. The stated objective at the time was to provide a payment and store-of-value means to many of the world's as of yet unbanked citizens. The project was widely viewed by state actors as incompatible with states' monetary policies and regulations[106] (and as such, it is being scaled down[107]). So far, it has had the merit of further bringing forward the debate of whether or not to issue state-backed digital currencies, whether these come in the form of a stablecoin or something else, see e.g. [68].

[105] https://www.diem.com/en-us/ (accessed 09/04/2021)

[106] https://www.wsj.com/articles/facebook-wanted-to-create-a-new-currency-it-wasnt-ready-for-the-backlash-11571242795 (accessed 09/04/2021)

[107] https://www.reuters.com/article/us-facebook-cryptocurrency-idUSKCN21Y277 (accessed 09/04/2021)

4

Technical standardization in Blockchain and DLT

4. Technical standardization in Blockchain and DLT

4.1. Technical standardization introduction

4.1.1. Technical standards

The European Regulation (EU) N°1025/2012 on European standardization[108] gives the following definition of a standard:

> *"a technical specification, adopted by a recognized standardization body, for repeated or continuous application, with which compliance is not compulsory [...]"*

Standards are meant to bring solutions to recurrent technical and business problems, on a broad scale, and may apply to products, services, and processes. The World Trade Organization[109] has listed a set of fundamental principles that international standards and standards development should adhere to in order to be adequate. These are:

- transparency of technical work programs,
- openness in participation,
- impartiality and consensus across all stakeholders in technical development,
- effectiveness and relevance in answering technical and market needs, and
- the inclusion of a dimension on facilitating developing countries' participation.

The benefits of applying technical standards are numerous:

Quality and security. Technical standards are developed primarily to solve problems and increase the quality of the target solution. A standardized product carries with it the knowledge of good practices from a large pool of experts.

Interoperability and trade facilitation. Standardized products support the use of common technical languages to describe problems, solutions, and requirements. Thus, they favor interoperability and exchange.

Competitiveness. Adhering to a recognized standard in a field gives a competitive edge, owing to the qualitative benefits that standards provide.

Efficiency. Standards are developed with a view towards bringing the most broadly applicable and effective solution in mind, while preserving a large degree of flexibility.

[108] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025

[109] https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm

4.1.2. Major international and European standards bodies

The overall worldwide standards landscape is quite complex, because it contains major international, regional and national standards bodies, in addition to thousands of industrial fora, consortia, associations etc. that develop technical specifications and other deliverables. Nevertheless, for the purpose of this document, six important bodies stand out, three at the international level and three at the European level.

The three most prominent international standards bodies are:

- the International Organization for Standardization (ISO);
- the International Electrotechnical Commission (IEC);
- the International Telecommunication Union's Telecommunication Standardization Sector (ITU-T).

The three official European Standardization Organizations (identified as such by Regulation (EU) N°1025/2012 on European standardization) are:

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

The governance system for ISO, IEC, CEN, and CENELEC organizes membership per state, while that of ITU and ETSI does so per organization. Thus, any given state involved in ISO, IEC, CEN, or CENELEC has one or more National Standards Bodies (NSBs) representing them within these organizations. Often, these national bodies are also in charge of developing national-level standards. In Luxembourg, the NSB is ILNAS (see Section 4.1.3), which is also a member of ITU-T and ETSI.

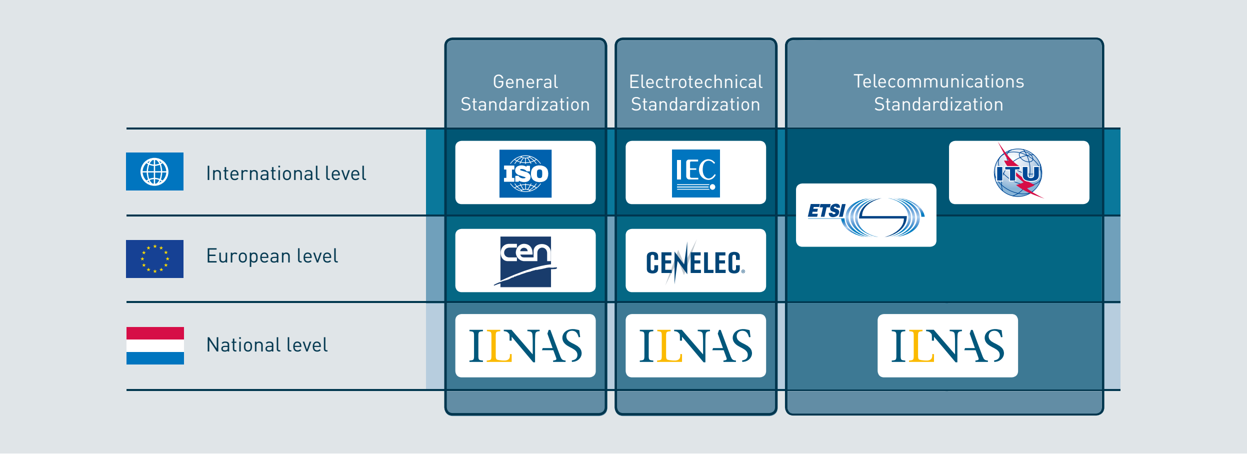


Figure 16: Relative positioning of the main standards developing organizations

4.1.3. ILNAS and ANEC GIE

ILNAS

ILNAS *(Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services)* is a public administration under the authority of the Minister of the Economy of the Grand Duchy of Luxembourg. Founded in 2008, ILNAS represents a network of competencies relating to quality, safety and conformity of products and services (see Figure 17), and its objective is to support national competitiveness.

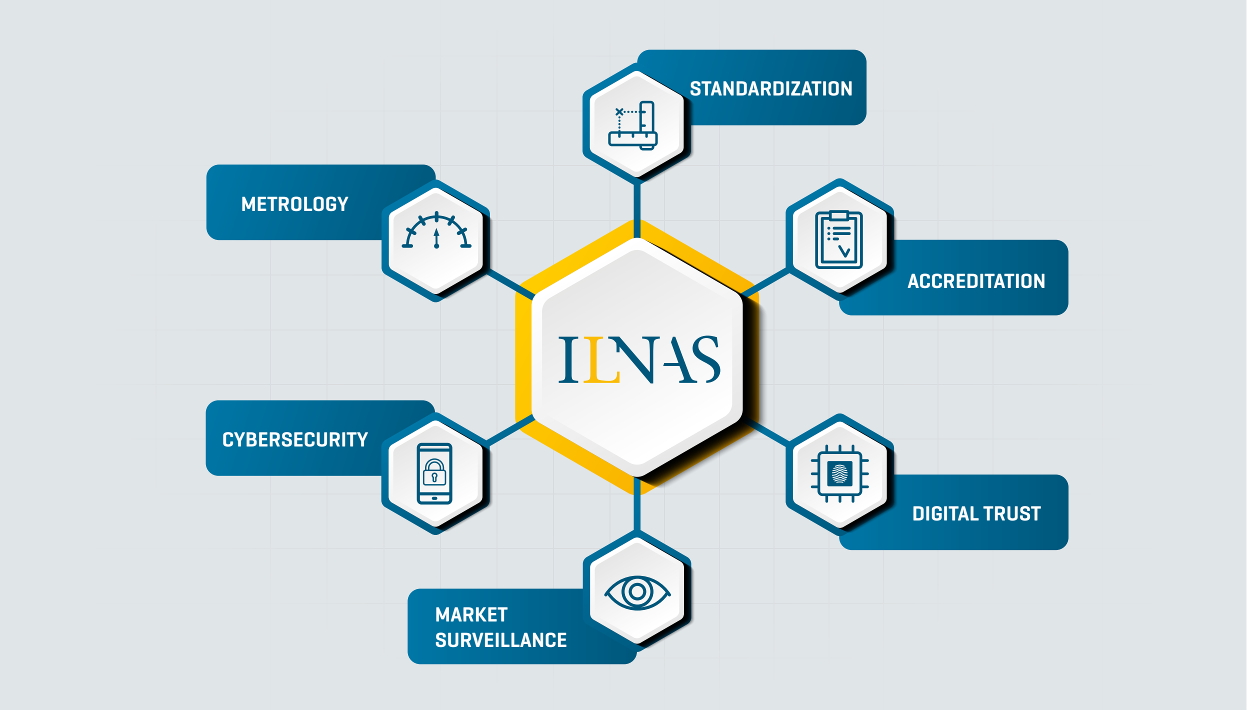


Figure 17: The departments of ILNAS

One of ILNAS' missions is to promote technical standardization. As such, it is the Grand Duchy's National Standards Body.

ILNAS organizes its standardization work according to the 2020-2030 national standardization strategy[110], and associated ICT[111], Construction[112], and Aerospace[113] national technical standardization policies. Overall, the objectives are to raise awareness on the use of technical standards, promote active participation in the development and publication of standards drafts, enhance Luxembourg's international visibility in standardization, and develop strong links between standardization, scientific research and education.

[110] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/strategie-normative-luxembourgeoise-2020-2030.html

[111] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2020-2025.html

[112] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-du-secteur-de-la-construction-2020-2025.html

[113] https://portail-qualite.public.lu/fr/publications/normes-normalisation/avis-officiels/politique-luxembourgeoise-pour-la-normalisation-technique-du-secteur-de-l-aerospatial-2021-2025.html

ANEC GIE

ANEC GIE *(Agence pour la normalisation et l'économie de la connaissance)* is an economic interest group whose partners are the Ministry of the Economy, the *Chambre des métiers* and the *Chambre de commerce*. One of its main roles is to support ILNAS in its standardization missions. In particular, it implements the 2020-2025 national standardization policy for ICT. In practice, this entails pursuing the following activities:

- Regularly informing the national market of the latest technical standardization developments;
- Actively promoting the use of standards and the benefits of participating in the standards development process;
- Animating trainings on technical standardization in relation to technologies of interest;
- Actively participating in national mirror committees for certain international technical committees;
- Representing Luxembourg in certain international and European technical committee meetings, and communicating the national position in these committees' ballots;
- Supporting ILNAS in the production of national deliverables, such as white papers, national technical standardization reports, topic-specific standards analyses, etc.;
- Supporting ILNAS in its efforts to strengthen the ties between technical standardization, scientific research, education, and innovation, namely through research programs between ILNAS and the University of Luxembourg[114], and participation in the MTECH Master's degree (Technopreneurship: mastering smart ICT, standardisation and digital trust for enabling next generation of ICT solutions[115]).

4.1.4. Participating in technical standardization

In its capacity of NSB for Luxembourg, ILNAS (along with the ANEC GIE) is the gateway to technical standardization for the country in ISO, IEC, CEN, and CENELEC.

Benefits

Participating in technical standards development has multiple advantages.

Gain advance knowledge on future specifications. Future products in your field may be influenced by a widely accepted standard. Advance knowledge of this aids in proactively adapting to the market.

Shape standards according to your needs and knowhow. Standards are a way to spread your ideas and requirements, not just as a way to remain competitive, but also to enhance the value of your expertise and making it known to a wide range of stakeholders.

Gain access to a strategic network of experts. Participating grants access to a larger pool of technical expertise, and knowing who works in standardization sheds further light on current and future interests of partners and competitors.

[114] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/normalisation-recherche.html

[115] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/education-normalisation.html

How to get involved in Luxembourg

ILNAS offers the possibility for nationally established companies to register actively participating delegates within ISO, IEC, CEN, and CENELEC technical committees free-of-charge. ILNAS also offers support and coaching to new delegates, in order to assist them in their standardization needs. Roles held by delegates can range from being a simple expert that comments and votes on projects to more involved tasks such as proposing new work items and leading the editing of projects. It only depends on the time one wishes to grant to these activities.

The full range of ILNAS' service related to technical standardization in support of the national market can be found on the *Portail Qualité*[116].

4.2. ISO and IEC Blockchain activities

4.2.1. The international technical committee ISO/TC 307 Blockchain and distributed ledger technologies

ISO/TC 307 *Blockchain and distributed ledger technologies*[117] was launched in 2017. Composed of 46 participating member states and 14 observing member states, its secretariat is under the administrative responsibility of Standards Australia, the Australian national standards body. Its scope is quite concise: "Standardisation of blockchain technologies and distributed ledger technologies"[118].

Luxembourg became a participating member of this technical committee in 2017; the national mirror committee[119] is currently composed of 13 delegates and its development is overseen by a dedicated resource within ANEC GIE.

Since its launch, TC 307 has undergone a few structural changes. It currently has the following groups doing technical work under its administrative responsibility:

WG 1 Foundations

This working group handles all foundational work involving Blockchain and DLT. Thus, it covers topics such as basic definitions of the overall technology, ontology work, and fundamental system architectures.

WG 2 Security, privacy and identity and JWG 4 Joint ISO/TC 307 –ISO/IEC JTC 1/SC 27 WG on security, privacy and identity for Blockchain and DLT

Information security, privacy and personal data protection, and questions related to identification are central to Blockchain technologies. Thus, specific working groups are currently dedicated to these. At present, one is purely under the control of TC 307, and another is a joint working group with the technical sub-committee ISO/IEC JTC 1/SC 27 *Information security, cybersecurity and privacy protection*[120], which develops standards "for the protection of information and ICT" horizontally across namely all subcommittees of ISO/IEC JTC 1 *Information technology*[121].

[116] https://portail-qualite.public.lu/fr/normes-normalisation.html

[117] https://www.iso.org/committee/6266604.html

[118] Its active business plan can be found at https://isotc.iso.org/livelink/livelink/fetch/2000/2122/687806/ISO_TC_307__Blockchain_and_distributed_ledger_technologies_.pdf?nodeid=19772644&vernum=-2 (last accessed 09/04/2021)

[119] https://portail-qualite.public.lu/fr/normes-normalisation/secteurs/tic/blockchain.html

[120] https://www.iso.org/committee/45306.html

[121] https://www.iso.org/isoiec-jtc-1.html

WG 3 Smart contracts

This group focuses mainly on the definitions and specifications of the very specific Blockchain construct that is the smart contract, since these are at the heart of the expansion of Blockchain capabilities beyond simple transaction recording. Topics of interest also include certain aspects of smart contracts' relations to legal questions.

WG 5 Governance

WG 5 is dedicated to questions on governance of Blockchain systems. The decentralized nature of a distributed ledger introduces subtleties to organizational governance for instance in terms of accountability and decision authority.

WG 6 Use cases

Blockchain use cases are gathered and examined in this working group in order to describe and classify how blockchains are implemented and used in the field. Topics covered may be transversal to other groups' subjects of focus, such as data flows, examples of identifiers, etc.

SG 7 Interoperability

Interoperability between different blockchains and between blockchains and legacy systems is one of the greatest technical challenges to date. Thus, a study group is dedicated to this.

AhG 2 Guidance for auditing DLT systems

The decentralized nature of DLT creates specific challenges for auditing such systems. An ad hoc group was set up to tackle this question.

Finally, there is a joint working group with ISO/TC 46/SC 11 *Archives/records management*[122], under the latter's administrative responsibility:

[122] https://www.iso.org/committee/48856.html

JWG 1 Joint ISO/TC 46/SC 11 - ISO/TC 307 WG: Blockchain

This joint working group examines the possible uses of blockchains in record management systems and other connected topics.

The list of published and ongoing projects undertaken by TC 307 can be found in Table 4. For more details on the program of work, the reader can consult the technical committee's website[123].

WG	Project	Status
WG 1	ISO 22739:2020 *Blockchain and distributed ledger technologies — Vocabulary*[124]	Published, under revision
	ISO 22739 *Blockchain and distributed ledger technologies — Vocabulary*[125]	Ongoing (project to update 22739)
	ISO 23257 *Blockchain and distributed ledger technologies — Reference architecture*[126]	Ongoing
	ISO/TS 23258 *Blockchain and distributed ledger technologies — Taxonomy and Ontology*[127]	Ongoing
WG 2	ISO/TR 23642 *Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues*[128]	Ongoing
WG 3	ISO/TR 23455:2019 *Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*[129]	Published
	ISO/TS 23259 *Blockchain and distributed ledger technologies — Legally binding smart contracts*[130]	Ongoing
JWG 4	ISO/TR 23244:2020 *Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations*[131]	Published
	ISO/TR 23576:2020 *Blockchain and distributed ledger technologies — Security management of digital asset custodians*[132]	Published
	ISO/TR 23249 *Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management*[133]	Ongoing
	ISO/TR 23644 *Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM)*[134]	Ongoing
WG 5	ISO/TS 23635 *Blockchain and distributed ledger technologies — Guidelines for governance*[135]	Ongoing

Table 4: ISO/TC 307 published and ongoing projects (part 1)

[123] https://www.iso.org/committee/6266604/x/catalogue/p/0/u/1/w/0/d/0

[124] https://www.iso.org/standard/73771.html?browse=tc

[125] https://www.iso.org/standard/82208.html?browse=tc

[126] https://www.iso.org/standard/75093.html?browse=tc

[127] https://www.iso.org/standard/75094.html?browse=tc

[128] https://www.iso.org/standard/81772.html?browse=tc

[129] https://www.iso.org/standard/75624.html?browse=tc

[130] https://www.iso.org/standard/75095.html?browse=tc

[131] https://www.iso.org/standard/75061.html?browse=tc

[132] https://www.iso.org/standard/76072.html?browse=tc

[133] https://www.iso.org/standard/80805.html?browse=tc

[134] https://www.iso.org/standard/81773.html?browse=tc

[135] https://www.iso.org/standard/76480.html?browse=tc

WG 6	ISO/TR 3242 *Blockchain and distributed ledger technologies – Use cases*[136]	Ongoing
	ISO/TR 6039 *Blockchain and distributed ledger technologies - Identifiers of subjects and objects for the design of blockchain systems*[137]	Ongoing
	ISO/TR 6277 *Blockchain and distributed ledger technologies – Data flow model for blockchain and DLT use cases*[138]	Ongoing
JWG 1 (administered by ISO/TC 46/SC 11)	ISO/TR 24332 *Blockchain and Distributed Ledger Technology in relation to authoritative records, records systems, and records management*[139]	Ongoing

Table 4: ISO/TC 307 published and ongoing projects (part 2)

4.2.2. Other blockchain projects in ISO and IEC

Blockchain and distributed ledgers have potentially many applications. Thus, other ISO and/or IEC technical committees have taken an interest. Some examples of published or ongoing projects in other technical committees can be found in Table 5.

Committee	Project	Status
ISO/TC 68/SC 2 *Financial Services, security*[140]	ISO/TR 24374 *Information technology — Security techniques — DLT and Blockchain for Financial Services*[141]	Ongoing
ISO/TC 184/SC 4 *Industrial data*[142]	ISO 8000-117 *Data quality — Part 117: Application of ISO 8000-115 to Quality Blockchains*[143]	Ongoing
ISO/TC 154 *Processes, data elements and documents in commerce, industry and administration*[144]	ISO 19626-1:2020 *Processes, data elements and documents in commerce, industry and administration — Trusted communication platforms for electronic documents — Part 1: Fundamentals*[145]	Published
ISO/IEC JTC 1/SC 41 *Internet of things and digital twin*[146]	ISO/IEC TR 30176 ED1 *Internet of Things (IoT) - Integration of IoT and DLT/Blockchain: Use Cases*[147]	Ongoing

Table 5: Projects touching on blockchain and DLT in other ISO and/or IEC technical committees

[136] https://www.iso.org/standard/79543.html?browse=tc

[137] https://www.iso.org/standard/81978.html?browse=tc

[138] https://www.iso.org/standard/82158.html?browse=tc

[139] https://www.iso.org/standard/78465.html?browse=tc

[140] https://www.iso.org/committee/49670.html

[141] https://www.iso.org/standard/78510.html

[142] https://www.iso.org/committee/54158.html

[143] https://www.iso.org/standard/81208.html

[144] https://www.iso.org/committee/53186.html

[145] https://www.iso.org/standard/65536.html

[146] http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID:20486

[147] https://www.iec.ch/ords/f?p=103:38:300556391241056::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,104008

4.3. CEN and CENELEC Blockchain activities

4.3.1. The Focus Group on Blockchain and DLT and their white paper

In 2017, CEN and CENELEC created a Focus Group on Blockchain and DLT to assess Blockchain requirements for Europe. This Focus Group – since disbanded – published a white paper in 2018 “Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies”.

The white paper formulated a total of 26 recommendations. Topics identified as being of interest to the EU Single Market include, but are not limited to:

- Digital identity and electronic signatures,
- Data protection and integrity,
- Security,
- Cross border data-sharing, and
- Interoperability.

4.3.2. The European technical committee CEN/CENELEC/JTC 19 Blockchain and distributed ledger technologies

Following the publication of the focus group’s white paper (see Section 4.3.1), in January 2020 CEN/CENELEC established a new joint technical committee, CEN/CENELEC/JTC 19 *Blockchain and distributed ledger technologies*[148]. The main objective of this technical committee is to assess and fill Blockchain standardization needs for the European market. This includes adopting international standards - in particular, those that might be output by ISO/TC 307 (see Section 4.2.1) - as European standards and developing European standards from scratch to satisfy a specific European requirement, typically in support of EU Digital Single Market, and/or EU legislation.

The preliminary scope of this joint technical committee lists the following topics as being of interest:

- Organizational frameworks and methodologies, including IT management systems,
- Process and product evaluation schemes,
- Blockchain and distributed ledger guidelines,
- Smart technology and objects,
- Distributed computing devices, and
- Data services.

At the time of writing, CEN/CENELEC/JTC 19 has not yet established any working groups. However, it will soon adopt as a European standard the international standard ISO 22739:2020 *Blockchain and distributed ledger technologies — Vocabulary*.

[148] https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:2702172&cs=1465AF26367A9ECE85D149F31EF39162E

4.4. ETSI Blockchain activities

ETSI has an ongoing Industry Specification Group (ISG) on *Permissioned Distributed Ledgers*[149] (PDL). An ISG is a quickly set-up type of ETSI structure that produces deliverables related to a specific technology area. The deliverables are either informative reports (Group Reports) or recommendations (Group Specifications).

The PDL ISG takes the view that PDLs are the most adequate to address business, industry, and government use cases. Its objective is to create definitions for PDL common mechanisms, e.g. participating node validation, publication and execution of recorded operations, and creation of trusted links between ledgers, among others.

Published and ongoing work items can be found in Table 6.

Project	Status
ETSI GR PDL 001 V1.1.1 (2020-03) *Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies*[150]	Published
ETSI GR PDL 002 V1.1.1 (2020-11) *Permissioned Distributed Ledger (PDL); Applicability and compliance to data processing requirements*[151]	Published
ETSI GR PDL 003 V1.1.1 (2020-12) *Permissioned Distributed Ledger (PDL); Application Scenarios*[152]	Published
ETSI GR PDL 004 V.1.1. (2021-02) *Smart Contracts Permissioned Distributed Ledgers System Architecture and Functional Specification*[153]	Published
ETSI GS PDL 005 V1.1.1 (2020-03) *Permissioned Distributed Ledger (PDL); Proof of Concepts Framework*[154]	Published
ETSI GR PDL 006 *Inter-Ledger Interoperability*[155]	Ongoing
ETSI GR PDL 008 *Research and Innovation Landscape*[156]	Ongoing
ETSI GR PDL 009 *PDL for Federated Data Management*[157]	Ongoing
ETSI GR PDL 010 *Operations in Offline Mode*[158]	Ongoing

Table 6: Published and ongoing deliverables from ETSI's ISG PDL

[149] https://www.etsi.org/committee/1467-pdl

[150] https://www.etsi.org/deliver/etsi_gr/PDL/001_099/001/01.01.01_60/gr_PDL001v010101p.pdf

[151] https://www.etsi.org/deliver/etsi_gr/PDL/001_099/002/01.01.01_60/gr_PDL002v010101p.pdf

[152] https://www.etsi.org/deliver/etsi_gr/PDL/001_099/003/01.01.01_60/gr_PDL003v010101p.pdf

[153] https://www.etsi.org/deliver/etsi_gr/PDL/001_099/004/01.01.01_60/gr_PDL004v010101p.pdf

[154] https://www.etsi.org/deliver/etsi_gs/PDL/001_099/005/01.01.01_60/gs_PDL005v010101p.pdf

[155] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59251

[156] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=59474

[157] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=61975

[158] https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=62004

4.5. ITU-T Blockchain activities

4.5.1. The Focus Group on DLT (FG DLT)

ITU-T established a *Focus Group on DLT*[159], that ran from May 2017 to August 2019. An ITU-T focus group is an entity designed to study specific topics that are not immediately covered in established ITU-T study groups. Focus groups are fast to set up, and can choose the type of deliverables they wish to output. Those output by FG DLT are Technical Reports (informative) and Technical Specifications (containing guidance).

Per the FG DLT website, the purpose of FG DLT was to:

- *"identify and analyse DLT-based applications and services;*
- *draw up best practices and guidance which support the implementation of those applications and services on a global scale; and*
- *propose a way forward for related standardization work in ITU-T Study Groups."*

Since FG DLT was only recently terminated, and its output continues to serve in ongoing work, it remains relevant to describe in this report.

The group produced 8 publicly-available deliverables, listed below:

- Technical Specification FG DLT D1.1 *DLT terms and definitions*[160]
- Technical Report FG DLT D1.2 DLT *overview, concepts, ecosystem*[161]
- Technical Report FG DLT D1.3 DLT *standardization landscape*[162]
- Technical Report FG DLT D2.1 DLT *use cases*[163] *and use case file*[164]
- Technical Specification FG DLT D3.1 *DLT reference architecture*[165] *and platform mapping*[166]
- Technical Specification FG DLT D3.3 *Assessment criteria for DLT platforms*[167]
- Technical Report FG DLT D4.1 DLT *regulatory framework*[168]
- Technical Report FG DLT D5.1 *Outlook on DLTs*[169]

4.5.2. Study groups in ITU-T

Most Blockchain and/or distributed ledger activity in ITU-T is found in Study Groups 16 *Multimedia*[170], 17 *Security*[171], and 20 *IoT*, *smart cities & communities*[172]. Thus, we briefly describe these groups' overall work. However, some

[159] https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx

[160] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf

[161] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf

[162] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d13.pdf

[163] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf

[164] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.zip

[165] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d31.pdf

[166] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d31.zip

[167] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d33.pdf

[168] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d41.pdf

[169] https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d51.pdf

[170] https://www.itu.int/en/ITU-T/studygroups/2017-2020/16/Pages/default.aspx

[171] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx

[172] https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

specific items are found also in Study Groups 2 *Operational aspects*[173], 11 *Protocols and test specifications*[174] and 13 *Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures*[175]. A list of published and ongoing work across all of these groups can be found in Table 7.

SG 16 Multimedia

SG 16's work focuses on aspects related to multimedia, covering topics such as media coding, signal processing, human interfaces, e-services and other applications, and digital signage. It also coordinates this work with the other study groups.

Most of the work related to Blockchain technology currently in the pipeline involves specifying requirements for blockchains as supporting technologies for applications of interest to SG 16, e.g. in human factor services and surveillance.

SG 17 Security

The *Security* study group works on security standards in a cross-group manner to the other groups. Among the topics it covers one finds cybersecurity, security management, identity management, and privacy protection, along with some aspects of IoT application and services security, cloud computing, and big data analytics.

Since Blockchain technology is actively considered for its ability to provide decentralized trust, it holds a natural place in the field of information security. In this study group, the security of Blockchain systems themselves is mostly considered, rather than that of applications supported by blockchains.

SG 20 IoT, Smart cities & Communities

This study group handles the topic of the Internet of Things within ITU-T. Its scope includes architecture, interoperability, machine-to-machine communication and sensor networks. Its work initially originated in Smart city applications, but it now covers also industrial applications, and more generally connectivity of all aspects of society.

Blockchain work in this area focuses mostly on decentralization of IoT network management, dealing with topics such as data sharing, transacting, and self-organization.

Study group	Question	Project	Status
SG 2	Q5/2 *Requirements, priorities and planning for telecommunication/ ICT management and operation, administration and maintenance (OAM) Recommendations*	M.rmbs *Requirements for management of blockchain system*[176]	Ongoing
	Q7/2 *Interface specifications and specification methodology*	M.immbs *Information model for management of blockchain system*[177]	Ongoing
SG 11	Q14/11 *Testing of cloud, SDN and NFV*	Q.BaaS-iop-reqts *Interoperability testing requirements of blockchain as a service*[178]	Ongoing

Table 7: Published and ongoing blockchain and DLT work in ITU-T Study Groups (part 1)

[173] https://www.itu.int/en/ITU-T/studygroups/2017-2020/02/Pages/default.aspx

[174] https://www.itu.int/en/ITU-T/studygroups/2017-2020/11/Pages/default.aspx

[175] https://www.itu.int/en/ITU-T/studygroups/2017-2020/13/Pages/default.aspx

[176] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16434

[177] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16442

[178] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16510

SG 13	Q2/13 *Next-generation network (NGN) evolution with innovative technologies including software-defined networking (SDN) and network function virtualization (NFV)*	ITU-T Y.2342 (12/2019): *Scenarios and capability requirements of blockchain in next generation network evolution*[179]	Published
		Y.NRS-DLT-reqts *Scenarios and requirements of network resource sharing based on distributed ledger technology*[180]	Ongoing
	Q17/13 *Future Networks: Requirements and capabilities for computing including cloud computing and data handling*	ITU-T Y.3530 (09/2020): *Cloud computing - Functional requirements for blockchain as a service*[181]	Published
	Q22/13 *Networks beyond IMT2020: Emerging network technologies*	Y.SCid-fr *Requirements and converged framework of self-controlled identity based on blockchain*[182]	Ongoing
SG 16	Q5/16 *Artificial intelligence-enabled multimedia applications*	F.Supp-OCAIB *Overview of convergence of artificial intelligence and blockchain*[183]	Published
	Q12/16 *Intelligent visual systems and services*	F.BVSSI *Scenarios and requirements for blockchain in visual surveillance system interworking*[184]	Ongoing
	Q22/16 *Multimedia aspects of distributed ledger technologies and e-services*	ITU-T F.751.0 (08/2020): *Requirements for distributed ledger systems*[185]	Published
		ITU-T F.751.2 (08/2020): *Reference framework for distributed ledger technologies*[186]	Published
		ITU-T F.751.1 (08/2020): *Assessment criteria for distributed ledger technologies*[187]	Published
		F.DLT-FIN *Financial distributed ledger technology application guideline*[188]	Ongoing
		H.DLT-DE *Digital evidence services based on distributed ledger technologies*[189]	Ongoing
	Q24/16 *Human factors for intelligent user interfaces and services*	F.DLIM-AHFS *Requirements of the distributed ledger incentive model for agricultural human factor services*[190]	Ongoing
		F.DLS-SHFS *Requirements of distributed ledger systems (DLS) for secure human factor services*[191]	Ongoing
		F.DLT.HC *Requirements of distributed ledger technologies (DLT) for human-care services*[192]	Ongoing

Table 7: Published and ongoing blockchain and DLT work in ITU-T Study Groups (part 2)

[179] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14128&lang=en

[180] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16485

[181] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14404&lang=en

[182] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16491

[183] https://www.itu.int/itu-t/recommendations/rec.aspx?rec=14651

[184] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15290

[185] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14332&lang=en

[186] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14334&lang=en

[187] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14333&lang=en

[188] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16656

[189] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15071

[190] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15287

[191] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15286

[192] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15024

		F.DLT.PHR (ex F.DLT.SM.PHR) *Service models of distributed ledger technologies (DLT) for personal health records (PHRs)*[193]	Ongoing
		F.HFS-BC *Requirements and framework for blockchain-based human factor service models*[194]	Ongoing
SG 17	Q14/17 *Distributed Ledger Technology (DLT) security*	ITU-T X.1400 (10/2020): *Terms and definitions for distributed ledger technology*[195]	Published
		ITU-T X.1404 (10/2020): *Security assurance for distributed ledger technology*[196]	Published
		ITU-T X.1402 (07/2020): *Security framework for distributed ledger technology*[197]	Published
		ITU-T X.1401 (11/2019): *Security threats of distributed ledger technology*[198]	Published
		ITU-T X.1403 (09/2020): *Security guidelines for using distributed ledger technology for decentralized identity management*[199]	Published
		X.das-mgt *Security threats and requirements for data access and sharing management system based on distributed ledger technology*[200]	Ongoing
		X.sa-dsm *Security architecture of data sharing management based on the distributed ledger technology*[201]	Ongoing
		X.sc-dlt *Security controls for distributed ledger technology*[202]	Ongoing
		X.srcsm-dlt *Security Requirements for Smart Contract Management based on the distributed ledger technology*[203]	Ongoing
		X.srip-dlt *Security requirements for digital integrity proofing based on distributed ledger technology*[204]	Ongoing
		X.ss-dlt *Security services based on distributed ledger technology*[205]	Ongoing
		X.stov *Security threats to online voting using distributed ledger technology*[206]	Ongoing
		X.str-dlt *Security threats and requirements for digital payment services based on distributed ledger technology*[207]	Ongoing

Table 7: Published and ongoing blockchain and DLT work in ITU-T Study Groups (part 3)

[193] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15025

[194] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14770

[195] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14449&lang=en

[196] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14450&lang=en

[197] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14251&lang=en

[198] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14092&lang=en

[199] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14264&lang=en

[200] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14589

[201] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16776

[202] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15257

[203] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16774

[204] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14821

[205] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14374

[206] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14377

[207] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14372

		X.tf-spd-dlt *Technical framework for secure software programme distribution mechanism based on distributed ledger technology*[208]	Ongoing
SG 20	Q2/20 *Requirements, capabilities and architectural frameworks across verticals enhanced by emerging digital technologies*	Y.IoT-BC-reqts-cap *IoT requirements and capabilities for support of blockchain*[209]	Ongoing
	Q3/20 *IoT and SC&C architectures, protocols and QoS/QoE*	Y.4476 (ex Y.IoT-rf-dlt) *OID-based resolution framework for transaction of distributed ledger assigned to IoT resources*[210]	Published
		Y.dec-IoT-arch *Decentralized IoT communication architecture based on information centric networking and blockchain*[211]	Ongoing
	Q4/20 *Data analytics, sharing, processing and management, including big data aspects, of IoT and SC&C*	ITU-T Y.4560 (08/2020): *Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities*[212]	Published
		ITU-T Y.4561 (08/2020): *Blockchain-based data management for supporting Internet of things and smart cities and communities*[213]	Published
		ITU-T Y Suppl. 62 (07/2020): *Overview of blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects*[214]	Published
		ITU-T Y.4464 (01/2020): *Framework of blockchain of things as decentralized service platform*[215]	Published
		Y.BC-SON *Framework of blockchain-based self-organization networking in IoT environments*[216]	Ongoing
		Y.blockchain-terms *Vocabulary for blockchain for supporting Internet of things and smart cities and communities in data processing and management aspects*[217]	Ongoing
		Y.IoT-BoT-peer *Capability and functional architecture of peer of blockchain of things*[218]	Ongoing
	Q7/20 *Evaluation and assessment of Smart Sustainable Cities and Communities*	ITU-T Y.4907 (08/2020): *Reference architecture of blockchain-based unified KPI data management for smart sustainable cities*[219]	Ongoing

Table 7: Published and ongoing blockchain and DLT work in ITU-T Study Groups (part 4)

[208] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14590

[209] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16859

[210] https://www.itu.int/ITU-T/recommendations/rec.aspx?id=14578&lang=en

[211] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=14650

[212] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14379&lang=en

[213] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14380&lang=en

[214] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14369&lang=en

[215] https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14167&lang=en

[216] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=15093

[217] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16679

[218] https://www.itu.int/itu-t/workprog/wp_item.aspx?isn=16863

[219] https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14949

4.5.3. Other initiatives in ITU-T

In January 2020, in a partnership with Stanford University, ITU-T launched the Digital Currency Global Initiative[220]. The broad objective is to study the framework and feasibility of deploying digital currencies, from the technical, regulatory and standardization standpoints, among others. The scope of digital currencies includes, but is certainly not limited to, currencies based on Blockchain and distributed ledger technologies, and stablecoins. There are three points of focus in the standardization track:

- Architecture, Interoperability Requirements and Use Cases,
- Policy and Governance, and
- Security and Assurance.

More details can be found in the initiative's terms of reference[221].

[220] https://www.itu.int/en/ITU-T/extcoop/dcgi/Pages/default.aspx

[221] https://www.itu.int/en/ITU-T/extcoop/dcgi/Documents/Digital%20Currency%20Global%20Initiative-ConceptNote-V4.pdf

4.6. Other sources of Blockchain standards, specifications, and guides

A great deal of international effort exists on the topic of Blockchain and DLT. Below is a non-exhaustive list of some of the most important other bodies that aim to provide technical specifications or technical reports comparable in intent to standards documents. Conditions on the documents' accessibility vary.

4.6.1. The Institute of Electrical and Electronics Engineers (IEEE)

IEEE (the Institute of Electrical and Electronics Engineers)[222] is a worldwide professional association for electronic and electrical engineering. As a part of its activities, it publishes technical standards in these fields, via the IEEE Standards Association (IEEE SA)[223]. Specific domains range from aerospace electronics, to transportation, through computer technology and energy. They also have work on Blockchain.

The IEEE Blockchain Initiative[224] has been active since January 2018. Among its subcommittees, one finds a group dedicated to blockchain standardization, collaborating closely with IEEE SA. As of February 2021, there are five published standards, and more than fifty standards under development. Topics of interest include:

- cryptocurrency exchanges,
- data formats,
- blockchain-based IoT,
- anti-corruption and anti-money laundering,
- payments and digital assets, and
- e-health.

4.6.2. The Enterprise Ethereum Alliance (EEA)

The Enterprise Ethereum Alliance[225] promotes the development and deployment of the Ethereum blockchain and related technologies. Organized in Interest Groups and Working Groups, it publishes and updates open technical specifications for Ethereum technology to be employed in an enterprise setting. It is based in the US, but has regional representation in Europe and in Asia.

It currently has four specifications[226] on Ethereum clients, Ethereum-based permissioned blockchains, and architecture.

[222] https://www.ieee.org/

[223] https://standards.ieee.org/

[224] https://blockchain.ieee.org/standards

[225] https://entethalliance.org/

[226] https://entethalliance.org/technical-specifications/

4.6.3. The National Institute of Standards and Technology (NIST)

The United States of America's National Institute of Standards and Technology (NIST) is a US government agency under the authority of the Department of Commerce[227]. Its mission is to provide technology standards in support of the US economy, in a broad set of domains including communications, cybersecurity, forensics, metrology, statistics, and others. NIST has been examining Blockchain technology since at least 2018[228].

While there are so far no deliverables containing technical recommendations, NIST's Blockchain project has published five technical reports and guidelines covering Blockchain generalities, identity management, industrial applications, and tokens.

4.6.4. The InterWork Alliance (IWA)

The InterWork Alliance (IWA)[229] is an industrial consortium based in the US, with world-wide membership. It has as a mission to promote the wider use of digital tokens as a means of value exchange, through decentralized transacting. A token is just a digital representation of a value, and many such existing tokens are Blockchain-or-DLT-supported.

As of February 2021, the IWA had published one technical specification on token taxonomy[230].

4.6.5. The International Association for Trusted Blockchain Applications (INATBA)

The International Association for Trusted Blockchain Applications (INATBA)[231] is a Belgium-based non-profit association of companies worldwide, launched in 2019 in cooperation with the European Commission. Its objectives are to promote the adoption of Blockchain and DLT technology, in particular through facilitating dialogue with public sector bodies and regulators. It is further subdivided into Advisor Bodies, Working Groups, and Committees. One such Committee is the Standardization committee. Sectoral topics of interest include governance, climate, education, healthcare, interoperability, finance, data protection and identity, just to name a few.

As of February 2021, INATBA has published five reports[232] on Blockchain and data protection regulations, decentralized identity, and unique object identifiers.

[227] https://www.commerce.gov/

[228] https://www.nist.gov/blockchain

[229] https://interwork.org/

[230] https://interwork.org/resources/technical-specifications/

[231] https://inatba.org/

[232] https://inatba.org/news/

Conclusion and outlook

This National Technical Standardization Report on Blockchain technology and technical standardization has the objective to remind the national market, after the 2018 Blockchain white paper [1], of the opportunities to seize in terms of using technical standards and participating in the standards development process of this still-new, and very promising field. The report first gives an overview of Blockchain concepts and some prominent players, before then describing European initiatives and multiple applications, and finally painting the picture of the overall Blockchain standardization landscape.

Standardization has a considerable role to play to support a technology's adoption, and even make it mainstream. Through the application of standards, businesses and technologists can find common ground, encouraging interoperability and building new market bridges. Thus, one of ILNAS' missions, as stated in the Luxembourg Standardization Strategy 2020-2030[233], is to actively promote the use of standards as they are published, to benefit from these effects as early as possible. To this end, ILNAS communicates regularly on standardization updates, disseminating the publication of new standards and technical committee activities. This is done through news items available on the *Portail-Qualité*[234], and technical reports (such as this one, or the 2020 report on the IoT[235]), white papers (such as the 2020 white paper on AI[236]), and national standards analyses (such as the Standards Analysis Smart Secure ICT, last updated in 2020[237]), developed with the support of ANEC GIE.

Even more importantly, creating the best conditions for national stakeholders to participate in standardization is also an ILNAS priority. Experts can gain valuable first-hand knowledge on projects which may very well become inevitable requirements later in time, discover and work with those shaping these documents, and even contribute to the drafts themselves. Hence, becoming a part of this process not only offers a window to the future, but also an additional chance to shape it in a way that benefits the national economy. ILNAS, with the support of ANEC GIE, can offer guidance and support to new delegates, should they wish to embark on this journey.

ILNAS can register national delegates in standardization committees from ISO, IEC, CEN, and CENELEC free of charge, so that they may make their voices heard and their ideas accepted in upcoming normative documents. In the context of Blockchain technologies, technical committees to consider for this are ISO/TC 307 *Blockchain and distributed ledger technologies*[238] and CEN/CENELEC/JTC 19 *Blockchain and distributed ledger technologies*[239]. Since Blockchain and DLT are still at an early stage in terms of standardization, now is the best time to act on this opportunity.

[233] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/strategie-normative-luxembourgeoise-2020-2030.pdf

[234] https://portail-qualite.public.lu/fr.html

[235] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/national-technical-standardization-report-iot-june-2020.pdf

[236] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2021/ilnas-white-paper-artificial-intelligence.pdf

[237] https://portail-qualite.public.lu/dam-assets/publications/normalisation/2020/smart-secure-ans-tic-september-2020.pdf

[238] https://www.iso.org/committee/6266604.html

[239] https://standards.cen.eu/dyn/www/f?p=204:22:0::::FSP_ORG_ID,FSP_LANG_ID:2702172,25&cs=1C5DF4D2E1D80EA24F5896718E20EA6F3

References

[1] ILNAS - ANEC GIE, "Blockchain and distributed ledgers: Technology, economic impact and technical standardization," ILNAS, v1.0, June 2018, https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-blockchain-dlt.html.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.

[3] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems, 4(3)*, 1982.

[4] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meikeljohn and G. Danezis, "SoK: Consensus in the age of blockchains," 2019, 10.1145/3318041.3355458.

[5] M. Pease, R. Shostak and L. Lamport, "Reaching agreement in presence of faults," *Journal of the ACM, 27(2)*, 1980.

[6] L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, 16(2), 1998.

[7] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," ACM transactions on Computer Systems, 20(4), 2002.

[8] Ethereum, "Ethereum," [Online]. Available: https://ethereum.org/. [Accessed 16 04 2021].

[9] C. Criddle, "Bitcoin consumes 'more electricity than Argentina'," BBC, [Online]. Available: https://www.bbc.com/news/technology-56012952. [Accessed 14 04 2021].

[10] Peercoin, "Peercoin," [Online]. Available: https://www.peercoin.net/. [Accessed 16 04 2021].

[11] E. 2, "Eth2," [Online]. Available: https://ethereum.org/en/eth2/. [Accessed 22 03 2021].

[12] S. Dziembowski, S. Faust, V. Kolmogorov and K. Pietrzak, "Proofs of space," *Proceedings of CRYPTO 2015, Part II*, Springer, 2015.

[13] Burst, "The Linux of blockchain," [Online]. Available: https://www.burst-coin.org/. [Accessed 16 04 2021].

[14] S. Park, A. Kwon, J. Alwen, G. Fuchsbauer, P. Gazi and K. Pietrzak, "SpaceMint: A Cryptocurrency Based on Proofs of Space," Cryptology ePrint Archive report 2015/528, 2015.

[15] M. Vukolic, "The quest for scalable blockchain fabric: proof-of-work vs. BFT replication," International Workshop on Open Problems in Network Security, Springer, 2015.

[16] I. Eyal and E. Gün Sirer, "Majority is not enough: Bitcoin mining is vulnerable," Financial Cryptography and Data Security - 18th international conference 2014, Springer.

[17] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert and P. Saxena, "A secure sharding protocol for open blockchains," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016.

[18] B. Rancea, "What is Ethereum Governance? Complete Beginner's Guide," [Online]. Available: https://unblock.net/what-is-ethereum-governance/. [Accessed 16 04 2021].

[19] J. A. Kroll, I. C. Davey and E. W. Felten., "The economics of Bitcoin mining," *Workshop on the Economics of Information Security, volume 2013*, 2013.

[20] N. Szabo, "Formalizing and securing relationships on public networks," First Monday 2(9), 1997.

[21] R. G. Brown, "The Corda Platform: An Introduction," https://www.r3.com/wp-content/uploads/2019/06/corda-platform-whitepaper.pdf, May, 2018. [Retrieved 08 04 2021].

[22] D. Ongaro and J. Ousterhout, "In Search of an Understandable Consensus Algorithm," *Proceedings of USENIX Annual Technical Conference 2014*, 2014.

[23] "IOTA," [Online]. Available: https://www.iota.org/. [Accessed 11 12 2019].

[24] S. Popov, H. Moog, D. Camargo, A. Capossele, V. Dimitrov, A. Gal, A. Greve, B. Kusmierz, S. Mueller, A. Penzkofer, O. Saa, W. Sanders, L. Vigneri, W. Welz and V. Attias, The Coordicide, The IOTA Foundation, January 2020.

[25] M. Del Castillo, "Forbes Blockchain 50, 2021," [Online]. Available: https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/?sh=8e354c1231cb . [Accessed 16 04 2021].

[26] ILNAS - ANEC GIE, "ILNAS White Paper ARTIFICIAL INTELLIGENCE: Technology, use cases and applications, trustworthiness and technical standardiaztion, v1.1," ILNAS, 2021, https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-artificial-intelligence-and-technical-standardization.html.

[27] ILNAS - ANEC GIE, "White Paper INTERNET OF THINGS: Technology, economic view and technical standardization, v1.0," ILNAS, 2018, https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/ilnas-white-paper-iot.html.

[28] K. Salah, M. Ur Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, Volume 7, 2019.

[29] D. Tapscott and A. Vinod, "Distributed Artificial Intelligence," Blockchain Research Institute, 2019.

[30] T. Lyons and L. Courcelas, "Convergence of Blockchain, AI, and IoT, v1.1," European Blockchain Observatory and Forum, 2020.

[31] P. Treleaven and B. Batrinca, "Algorithmic Regulation: Automating Financial Compliance Monitoring and Regulation Using AI and Blockchain," CAPCO Institute of Financial Transformation, n. 45, pp. 14-21, 2017.

[32] N. Mengidis, T. Tsikrita, S. Vrochidis and I. Kompatsiaris, "Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities," Information and Security, vol. 43, N. 1, 2019.

[33] D. Nguyen, M. Ding, P. Pathirana and A. Seneviratne, "Blockchain and AI-based Solutions to Combat Coronavirus (COVID-19)-like Epidemics: A Survey," preprint available online at https://www.techrxiv.org/articles/preprint/Blockchain_and_AI-based_Solutions_to_Combat_Coronavirus_COVID-19_-like_Epidemics_A_Survey/12121962/1, 2020.

[34] ILNAS - ANEC GIE, "INTERNET OF THINGS National technical standardization report, v1.0," ILNAS, 2020, https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/national-technical-standardization-report-iot-june-2020.html.

[35] EU Blockchain Observatory and Forum, "Convergence of Blockchain, AI and IoT, v1.1," EU Blockchain Observatory and Forum, 2020.

[36] O. Novo, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," *Journal of Internet of Things Class Files, Vol. 14, No. 8, 2018*, 2018.

[37] H. Lui, D. Han and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT," IEEE Access, *Special Section on Blockchain-enabled trustworthy systems, 2020*, 2020.

[38] I. Mistry, S. Tanwar, S. Tyagi and N. Kumar, "Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing 135 (2020)*, 2020.

[39] A. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A Decentralized Privacy-Preserving Healthcare for IoT," Sensors 2019, 19, 2019.

[40] D. Tosh, S. Shetty, P. Foytik, C. Kamhoua and L. Njilla, "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud," *11th IEEE International Conference on Cloud Computing (CLOUD), 2018*, 2018.

[41] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat and L. Njilla, "ProvChain: A Blockchain-Based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," *IEEE/ACM 17th International Symposium on Cluster, Cloud and Grid Computing (CCGRID)*, 2017.

[42] B. Ravishankar, P. Kulkarni and M. Vishnudas, "Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments," *2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI)*, 2020.

[43] S. Xie, W. Chen, Z. Zheng and J. Wu, "Blockchain for Cloud Exchange: A Survey," *Computers and Electrical Engineering, 81, 2019*, 2019.

[44] Lightning Network, "Lightning Network," [Online]. Available: https://lightning.network/. [Accessed 16 04 2021].

[45] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-chain Instant Payments," https://lightning.network/lightning-network-paper.pdf, 2016.

[46] Bitcoin Wiki, "Lightning network," [Online]. Available: https://en.bitcoin.it/wiki/Lightning_Network. [Accessed 16 04 2021].

[47] A. Whitten and J. Tygar, "Why Johnny can't encrypt," Proceedings of the 8th conference on USENIX Security Symposium, 1999.

[48] "EU Blockchain Observatory and Forum," [Online]. Available: https://www.eublockchainforum.eu/. [Accessed 31 03 2021].

[49] "Top 100 cryptocurrencies in market capitalization," [Online]. Available: https://coinmarketcap.com/. [Accessed 16 04 2021].

[50] "diem," [Online]. Available: https://www.diem.com/en-us/. [Accessed 31 03 2021].

[51] C. Goforth, "What the COVID-19 pandemic means for blockchain and crypto," [Online]. Available: https://cointelegraph.com/news/what-the-covid-19-pandemic-means-for-blockchain-and-crypto. [Accessed 16 04 2021].

[52] R. van Hoek and M. Lacity, "How the Pandemic Is Pushing Blockchain Forward," [Online]. Available: https://hbr.org/2020/04/how-the-pandemic-is-pushing-blockchain-forward. [Accessed 16 04 2021].

[53] L. Biscotti, "Blockchain Accelerates Amid Covid-19 Pandemic," [Online]. Available: https://www.forbes.com/sites/louisbiscotti/2020/08/18/blockchain-accelerates-amid-covid-19-pandemic/?sh=40c3ac772c0c. [Accessed 16 04 2021].

[54] H. Dyer, "The story of Worldometer, the quick project that became one of the most popular sites on the internet," [Online]. Available: https://www.newstatesman.com/science-tech/coronavirus/2020/05/story-worldometer-quick-project-became-one-most-popular-sites. [Accessed 16 04 2021].

[55] A. Banafa, "Blockchain Technology and COVID-19," [Online]. Available: https://www.bbvaopenmind.com/en/technology/digital-world/blockchain-technology-and-covid-19/. [Accessed 16 04 2021].

[56] E. F. F., "COVID-19 and Digital Rights," [Online]. Available: https://www.eff.org/issues/covid-19. [Accessed 16 04 2021].

[57] H. Zu, L. Zhang, O. Onireti, Y. Fang, W. Buchanan and M. Ali Imran, "BeepTrace: Blockchain-enabled Privacy-preserving Contact Tracing for COVID-19 Pandemic and beyond," https://arxiv.org/pdf/2005.10103.pdf, 2020.

[58] M. Kritikos, "Ten technolgies to fight coronavirus," European Parliament Research Service, 2020.

[59] A. Kalla, T. Hewa, R. Mishra, M. Yliantilla and M. Liyanage, "The Role of Blockchain to Fight Against COVID-19," IEEE Engineering Management Review, Vol. 48, Issue 3, Q3, 2020.

[60] M. Cerullo, "Emergency medical technicians are quitting their jobs — COVID-19 makes it too dangerous," [Online]. Available: https://www.cbsnews.com/news/ems-workers-retiring-higher-rates-coronavirus-pandemic/. [Accessed 16 04 2021].

[61] D. Tapscott and A. Tapscott, "Blockchain Solutions in Pandemics," Blockchain Research Institute, 2020.

[62] Q. Shang and A. Price, "A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects," *Innovations: Technology, Governance, Globalization (2019)*.

[63] M. Themistocleous, "Blockchain Technology and Land Registry," *The Cyprus Review, vol. 30:2, 2018*.

[64] J. Vos, "Blockchain-based land registry: Panacea, illusion, or something in-between?," *7th Annual Publication of the European Land Registry Association, 2017*.

[65] R. Bennet, T. Miller, M. Pickering and A. Kara, "Hybrid Approaches for Smart Contracts in Land Administration: Lessons from Three Blockchain Proofs-of-Concept," *Land 2021, 10(2), 2021*.

[66] A. Moin, K. Seqniki and E. Gun Sirer, "SoK: A Classification Framework for Stablecoin Designs," *International Conference on Financial Cryptography and Data Security, FC 2020, Springer, 2020*.

[67] M. Mita, K. Ito, S. Ohsawa and H. Tanaka, "What is Stablecoin?: A Survey on Price Stabilization Mechanisms for Decentralized Payment Systems," *2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), 2019*.

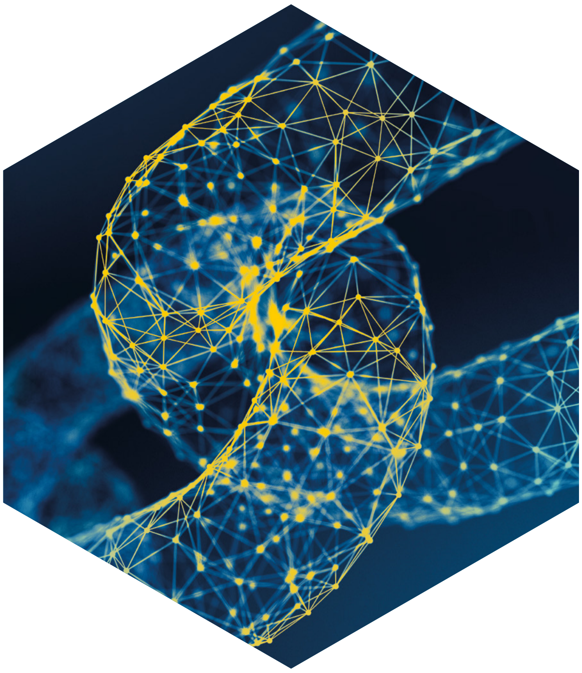
[68] Bank for International Settlements, "Central bank digital currencies: foundational principles and core features," Bank for International Settlements, 2010.

[69] R. Zhang and B. Preneel, "Lay down the common metrics: Evaluating proof-of-work consensus protocols' security," IEEE Symposium on Security and Privacy 2019.

[70] C. Dwork and M. Naor, "Pricing via processing, or, combatting junk mail," CRYPTO '92, Advances in Cryptology, LNCS, Springer, 1992.

[71] IOTA, "Academic papers," [Online]. Available: https://www.iota.org/research/academic-papers. [Accessed 16 04 2021].

[72] E. Classic, "Ethereum Classic," [Online]. Available: https://ethereumclassic.org/. [Accessed 16 04 2021].



June 2021 · NATIONAL TECHNICAL STANDARDIZATION REPORT · BLOCKCHAIN AND DISTRIBUTED LEDGERS · Version 1.0 · © ILNAS/ANEC · ISBN 978-99987-869-0-5

Institut Luxembourgeois de la
Normalisation, de l'Accréditation, de la
Sécurité et qualité des produits et services

Agence pour la Normalisation
et l'Economie de la Connaissance

Southlane Tower I · 1, avenue du Swing · L-4367 Belvaux · Tel. : (+352) 24 77 43 -70 · Fax : (+352) 24 79 43 -70 · E-mail : info@ilnas.etat.lu

www.portail-qualite.lu