ILNAS

White Paper

BLOCKCHAIN
AND DISTRIBUTED LEDGERS

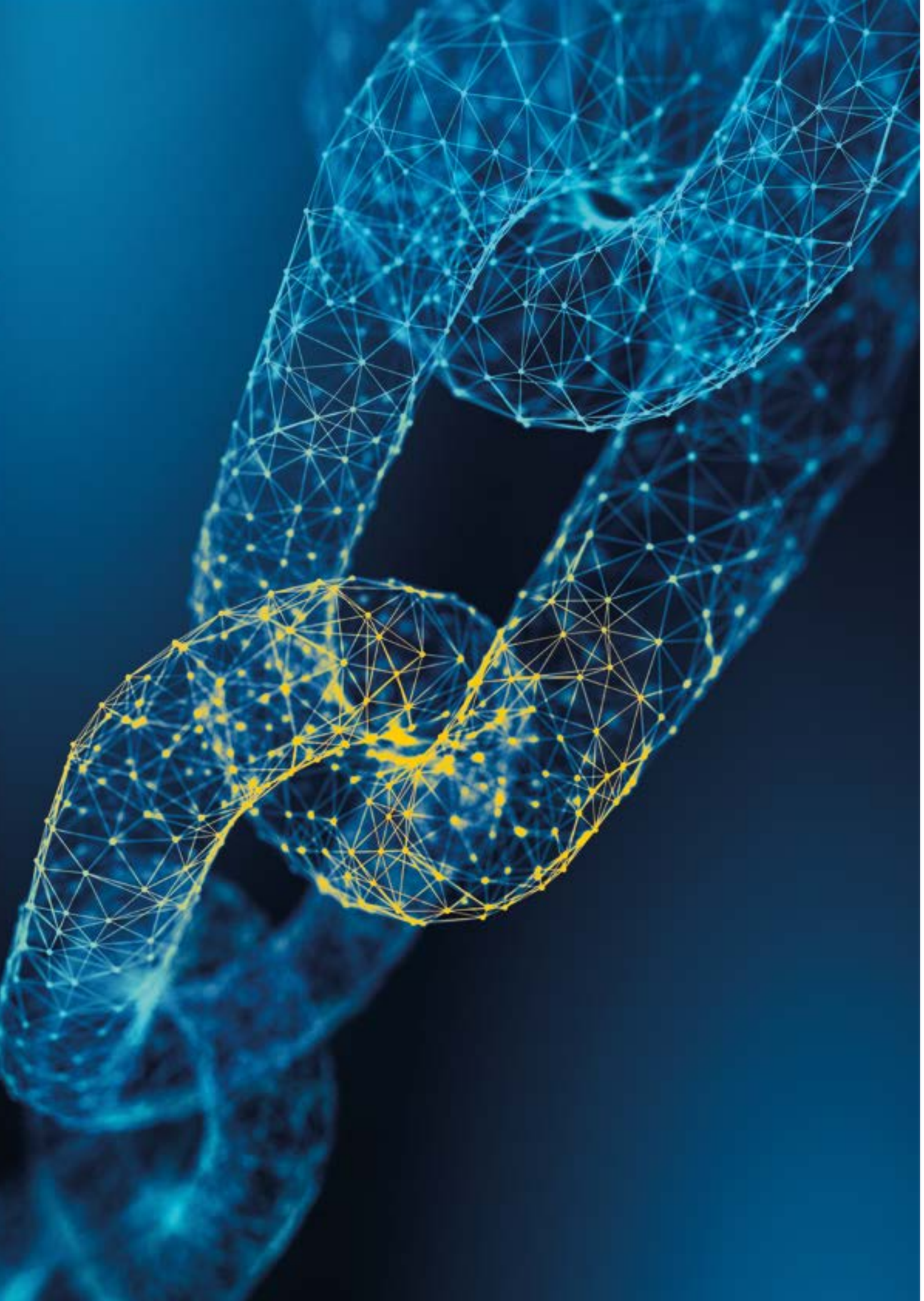
TECHNOLOGY, ECONOMIC IMPACT AND TECHNICAL STANDARDIZATION

Version 1.0 · June 2018

ANEC

Avec le support de :

LE GOUVERNEMENT
DU GRAND DUCHE DE LUXEMBOURG
Ministère de l'Économie



White Paper

BLOCKCHAIN
AND DISTRIBUTED LEDGERS

TECHNOLOGY, ECONOMIC IMPACT AND
TECHNICAL STANDARDIZATION

Version 1.0 · June 2018

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

Avec le support de :

LE GOUVERNEMENT
DU GRAND DUCHE DE LUXEMBOURG
Ministère de l'Économie

Information and Communication Technologies (ICT) have become an integral part of our economy and have assumed a predominant role in our lives. The unprecedented growth of these technologies and their interdisciplinary applications are making an impact across various economic sectors, around the world. Luxembourg is increasingly harnessing these technological developments to achieve positive transformation. Our approach to this transformation has been holistic in the sense that it not only covers strategic adoption but also building appropriate skills, ecosystems, infrastructure, policy as well as support, to ensure sustained future development.

Recently, blockchain and distributed ledger technologies (DLT) have attracted attention of various stakeholders globally, primarily because they are considered to have a potential to create various avenues for innovation, transformation and economic growth. These technologies are undergoing various developments. For instance, although bitcoin and other cryptocurrencies were originally widely known, the underlying technology that could facilitate trust, transparency, traceability and immutability, is gaining increasing attention. Similarly, while traditional blockchains were designed to be public and open, private and permissioned platforms that could transform business processes and provide decentralized enterprise applications are being developed. With enormous enthusiasm and effort from the market, Luxembourg is already establishing itself as a leader in this area, and our goal is to continue to tap the potential that these technologies offer.

In this context, it is important for market players to understand and gain comprehensive insights on the concepts, impact and developments relevant to these technologies. To this aim, this white paper describes the state-of-the-art and provides an analysis of blockchain and DLT from three different perspectives: basic concepts and technology, economic and business prospects, and technical standardization.

The first aspect clarifies fundamentals and provides a broad view of the technological landscape, including the requirements of digital trust as a cornerstone to resilient growth. The second aspect attempts to analyze the impact that this technology could have on the economy and on the businesses by means of case studies. The third aspect provides complete details on relevant work in technical standardization as a key source of knowledge that will establish common technical language, result in technology's convergence, and facilitate its continuous improvement.

ILNAS, the national standards body, is in charge of realizing the national technical standardization strategy, with a strong policy concerning the ICT sector. With associated research and education initiatives, this white paper is one among several projects that indicates the excellent path that ILNAS is taking to develop the necessary culture about ICT technical standardization at the national level.

Within this framework, Luxembourg will continue to consider technical standardization as a real force multiplier for the economy, for competitiveness, and specifically for the ICT sector.

Etienne Schneider

Deputy Prime Minister
Minister of the Economy

Acknowledgements

The working-group (WG) commissioned to prepare this white paper is:

Name of the contributor	Role	Institution/Organization
Mr. Mario GROTZ	Director General for Research, Intellectual Property and New Technologies	Ministry of the Economy
Mr. Michele GALLO	Director ICT Coordination	Ministry of the Economy
Mr. François THILL	Deputy Executive Advisor	Ministry of the Economy
Mr. Jean-Marie SPAUS	HPC Project Coordination	Ministry of the Economy
Mr. Daniel LIEBERMANN	Director, Directorate Logistics	Ministry of the Economy
Ms. Françoise LINERS	Director Life Sciences & Health Technologies	Ministry of the Economy
Mr. Jean-Marie REIFF	Director	ILNAS
Dr. Jean-Philippe HUMBERT	Deputy Director	ILNAS
Dr. Johnatan PECERO	Head of Standardization Department	ANEC G.I.E.
Dr. Ravi JHAWAR	Project Officer	ANEC G.I.E.
Mr. Nicolas DOMENJOUD	Project Officer	ANEC G.I.E.
Mr. Benoit POLETTI	General Director	Incert G.I.E.
Mr. Nasir ZUBAIRI	Co-founder, CEO	Luxembourg House of Financial Technology

This working-group would like to thank all the people who have helped and supported us, in different ways, in developing this white paper:

- Ms. Marianne HOFFMANN, Ministry of the Economy
- Mr. Lex KAUFHOLD, Ministry of the Economy
- Dr. ir. R.M. van WESSEL, Apexis Information Solutions
- Mr. Thibault CHOLLET, Deloitte Luxembourg
- Ms. Emeline BES, Deloitte Luxembourg
- Mr. Gaëtan PRADEL, Incert G.I.E.
- Mr. Marco HOUWEN, Infrachain a.s.b.l.
- Dr. Cyril CASSAGNES, Infrachain a.s.b.l.
- Mr. Said FIHRI, KPMG Luxembourg
- Mr. Romain FOURDIN, KPMG Luxembourg
- Dr. Pascal ROGIEST, LuxTrust S.A.
- Mr. Povilas ZINYS, LuxTrust S.A.

Table of contents

	Acknowledgements	**7**
	List of Figures	**10**
	List of Tables	**11**
	Introduction	**13**
1.	**Blockchain – A conceptual overview**	**17**
1.1	**How blockchain works**	**18**
1.2	**Network model**	**19**
1.3	**Blockchain as a database structure**	**20**
1.3.1	Data storage and management	20
1.3.2	Blockchain database structure and decentralization	21
1.3.3	Comparing attributes of traditional blockchain, distributed and decentralized databases	22
1.4	**Permissioned and permissionless blockchains**	**23**
1.5	**Consensus methods**	**25**
1.5.1	Proof-of-Work (PoW)	25
1.5.2	Proof-of-Stake (PoS)	26
1.5.3	Byzantine fault tolerance	27
1.5.4	Proof-of-Elapsed-Time (PoET) and Federated Byzantine Agreement (FBA)	28
1.6	**Smart contracts**	**30**
1.6.1	Introduction to smart contracts	30
1.6.2	Smart contracts and blockchains	30
2.	**Blockchain technology landscape analysis**	**33**
2.1	**High-level analysis of blockchain platforms**	**33**
2.2	**Hyperledger**	**35**
2.2.1	Hyperledger frameworks and tools	36
2.2.2	Hyperledger membership analysis	36
2.2.3	Hyperledger architecture and workflow	37
2.3	**Ethereum**	**40**
2.3.1	Background	40
2.3.2	Technical details on core Ethereum components	41
2.4	**Stellar**	**44**
2.4.1	Basic concepts, Stellar network, and Stellar.org	45
2.4.2	Anchors in Stellar network	46
2.4.3	Sending and receiving payments	47
2.4.4	Use cases	49
2.5	**Insights on blockchain related initiatives**	**50**
2.6	**Blockchain and Smart ICT**	**55**
2.6.1	Cloud computing	55
2.6.2	Big data and analytics	56
2.6.3	Internet of Things (IoT)	59

3.	**Blockchain and digital trust**	**63**
3.1	**Security**	**63**
3.1.1	Security risks to core blockchain operations	63
3.1.2	Risks due to smart contracts	64
3.1.3	Blockchain and PKI	67
3.2	**Privacy**	**68**
3.2.1	Storing sensitive information off-chain	69
3.2.2	One-time addresses and stealth addresses	69
3.2.3	Mixing and coinjoin	70
3.2.4	Blockchain and GDPR	71
4.	**Economic impact analysis**	**75**
4.1	**Economic analysis (high-level view)**	**75**
4.1.1	The new notion of money, trust and transactions	77
4.1.2	Improved governance, traceability and transparency (secure data registry)	82
4.1.3	Enforcing agreements	84
4.2	**Case study 1 – Funds distribution**	**85**
4.2.1	Typical business model	85
4.2.2	Industry challenges	86
4.2.3	Blockchain-based solution(s) and relevant initiatives	88
4.2.4	Economic impact and business opportunities for the funds distribution industry	91
4.3	**Case study 2 – Logistics and supply chain management**	**93**
4.3.1	Typical business model	93
4.3.2	Industry challenges	95
4.3.3	Blockchain-based solution(s) and relevant initiatives	97
4.3.4	Economic impact and business opportunities for the supply chain and logistics sector	100
4.4	**Case study 3 – Digital identity and data exchange**	**102**
4.4.1	Typical business model	102
4.4.2	Industry challenges	103
4.4.3	Blockchain-based solution(s) and relevant initiatives	104
4.4.4	Economic impact and business opportunities for digital identity	106
5.	**Blockchain and DLT standardization**	**109**
5.1	**Background on technical standardization and the national context**	**109**
5.2	**ISO/TC 307 Blockchain and distributed ledger technologies**	**111**
5.2.1	Members of ISO/TC 307	111
5.2.2	Liaisons	112
5.2.3	Structure of the Committee	113
5.2.4	Standards under development	115
5.2.5	Luxembourg's ISO/TC 307 mirror committee	116
5.3	**ITU-T's Focus Group on the applications of DLT**	**116**
5.4	**CEN-CENELEC's Focus Group on blockchain and DLT**	**117**
5.5	**Standardization activities related to blockchain and digital trust**	**118**
5.6	**Standardization activities related to blockchain and Smart ICT**	**119**
5.6.1	Cloud computing	119
5.6.2	Internet of Things and Big Data	120
5.7	**Summary of blockchain and DLT standardization projects**	**121**
6.	**Outlook and conclusions**	**125**
	References	**127**

List of Figures

Figure 1	Process of creating and validating transactions in a blockchain	18
Figure 2	Different types of networked systems	19
Figure 3	From traditional centralized cloud computing ecosystem (left) to fully decentralized blockchain ecosystem (right)	21
Figure 4	Process of running a smart contract on blockchain	31
Figure 5	Hyperledger architecture	38
Figure 6	Typical workflow / process in Hyperledger	39
Figure 7	Stellar overview	45
Figure 8	Sending payment using Stellar	47
Figure 9	Receiving payment using Stellar	48
Figure 10	Timeline of formation of blockchain consortia	50
Figure 11	Geographical distribution of blockchain consortia	54
Figure 12	The sector(s) in which a country is leading blockchain consortium	54
Figure 13	IoT and blockchain (typical) system architecture	61
Figure 14	Aspects studied for each case study	76
Figure 15	Cryptocurrency market cap (bitcoin vs altcoin)	77
Figure 16	Cryptocurrency market cap (% share)	78
Figure 17	%Market share of cryptocurrency exchanges	78
Figure 18	Monthly blockchain funding (ICO vs VC)	79
Figure 19	Cumulative blockchain funding (ICO vs VC)	80
Figure 20	End-users can directly access central bank ledgers	81
Figure 21	Simplified view of the funds distribution value chain	85
Figure 22	High-level view on the challenges within funds distribution	87
Figure 23	Estimate of annual operational costs in Luxembourg	92
Figure 24	Simple schema of a supply chain with material, information and financial flows	93
Figure 25	Representative trade finance model within supply chain management	94
Figure 26	Revamped supply chain business model	97
Figure 27	Standardization organizations and their scope of influence	110
Figure 28	ISO/TC 307 membership	112
Figure 29	ISO/TC 307 liaisons	113
Figure 30	Evolution of ISO/TC 307 structure since its creation	114

List of Tables

Table 1	Comparison between traditional blockchain and distributed databases; derivation of desired properties for decentralized blockchain databases	22
Table 2	Comparison of private permissioned and public permissionless blockchain	23
Table 3	Blockchain design choices related to (de)centralization and the impact of each choice on the favourability of various properties	24
Table 4	Analysis of consensus models across several blockchain parameters	29
Table 5	Analysis of blockchain platforms	34
Table 6	Projects within Hyperledger umbrella	35
Table 7	Hyperledger membership analysis	37
Table 8	Ethereum development roadmap	40
Table 9	Account types in Ethereum; their properties and differences	42
Table 10	Denomination in Ethereum	43
Table 11	Anchors in Stellar network	46
Table 12	Notable blockchain consortia in non-finance sectors	51
Table 13	Big data and blockchain use cases	58
Table 14	Internet of Things and blockchain use cases	60
Table 15	Security risks in smart contracts	66
Table 16	Comparison between PKI and public and private blockchains	68
Table 17	Analysis of GDPR data subject rights in the context of blockchain	72
Table 18	Blockchain features vs potential economic, business and societal impact	76
Table 19	Benefits and risks of ICO	80
Table 20	Activities performed within each operational process (example)	86
Table 21	Potential business opportunities for market players in funds distribution	91
Table 22	Operational processes of trade finance within supply chain management	95
Table 23	Challenges in trade finance within supply chain management	96
Table 24	Operational trade finance processes in a transformed (blockchain-enabled) supply chain model	98
Table 25	Potential business opportunities with blockchain-enabled trade finance within supply chains	101
Table 26	Applicability of attributes of an identity system in a centralized system, public blockchain and permissioned blockchain	104
Table 27	Opportunities for different players in an identity ecosystem	107
Table 28	ISO/TC 307 projects under development	115
Table 29	ITU-T Focus Group DLT's working groups, their mission and expected deliverables	117
Table 30	ITU-T blockchain and DLT projects related to digital trust	119
Table 31	Summary of blockchain and DLT standardization projects	122

Introduction

The past few years have witnessed a major ICT innovation in the form of the blockchain technology. The core of this innovation revolves around the notion of a distributed ledger that allows a network of computers to jointly create, evolve and keep track of a database of records (e.g., business transactions), colloquially known as the blockchain [1]. Another innovation of this technology comprises an underlying protocol that allows users to reach consensus without having to trust each other [2].

Until recently, bitcoin was seen as the most prominent application of the blockchain technology [3] [4] [5]. However, it is just one application of this technology; the real potential of blockchain goes far beyond, with applications across various sectors including (but not limited to) supply chains, healthcare, banking, financial services, digital media, payments and industry 4.0. This disruptive potential has led to an unparalleled attention and growth, with contributions from industries, academia, start-ups as well as administrations from across the globe.

The goal of this white paper is to provide a comprehensive view of the developments around blockchain and distributed ledger technologies. To this aim, a systematic analysis of this domain is presented from three different perspectives: blockchain concepts and technology, economic and business impact, and technical standardization, so that the readers of this white paper could broadly answer to questions such as:

- How does blockchain work?
- What are the features, differences and similarities, in major blockchain platforms?
- How will blockchain affect different economic sectors?
- What are the benefits of adopting blockchain within a given business?
- What are the recent developments in blockchain technical standardization?
- Which set of standards are relevant?

To achieve such broad and comprehensive outcomes, the rest of this white paper is organized along the three-abovementioned perspectives as follows.

Holistic analysis of blockchain concepts and technology

- **Chapter 1** describes fundamentals of blockchain starting from a conceptual overview on how blockchain works, to network and data management models, and finally to consensus methods and the role of smart contracts.
- **Chapter 2** builds on the concepts introduced in Chapter 1 and provides technology analysis across three dimensions:
  - First, a high-level analysis of blockchain platforms is provided, then two popular general-purpose projects Hyperledger and Ethereum are discussed in detail, and finally a platform designed specifically for digital assets and payments – Stellar – is studied.
  - The second part of this chapter provides insights on various consortia that were formed by companies, research institutions, and governments as a means to realize their blockchain strategy.
  - The third, and the final, part of this chapter establishes the relationship between blockchain and Smart ICT topics namely Cloud computing, Internet of Things and Big data, to study blockchain from an overall ICT ecosystem point of view.
- **Chapter 3** provides an analysis of the digital trust aspects of the blockchain technology. In particular, the strengths and issues of blockchain in terms of security and privacy are studied.

Economic and business impact analysis

Chapter 4 first provides insights on the potential impact of blockchain on the economy at a high-level (e.g., expected change in GDP, market share of cryptocurrency exchanges, etc.). Second, to help businesses in making informed decisions on the use of blockchain, three economic sectors namely, funds distribution, logistics and supply chain management, and digital identity and data protection services are considered as case studies, and for each sector, the following information is provided:

- A simple **model** of typical **business characteristics** representing information such as involved actors (internal and external), roles, representative business transactions, estimation of the time and cost to complete a business transaction, and revenue streams.
- Potential **challenges** in the business (e.g., untrusted intermediaries), based on the above model.
- Analysis of how and whether **blockchain based solutions** address the identified challenges. In this context, relevant initiatives and their developments are highlighted.
- Finally, insights on potential **economic impact** and **business opportunities** (e.g., reduced amount of time in performing a transaction, cost savings) in using blockchain based solutions.

Advancements in technical standardization

Chapter 5 provides a systematic review of relevant technical standardization activities at the national, European and international levels. This review is presented in three parts:

- The first part focuses on the International Organization for Standardization's Technical Committee ISO/TC 307 since it is one of the most active in building standards for blockchain and DLT. After providing background on standardization organizations in general, the formal developments in ISO/TC307, starting from its inception until March 2018, are outlined. These developments are presented by providing details about ISO/TC307's members, liaisons, structure as well as the projects that are currently under development. Finally, details about Luxembourg's participation in this committee are highlighted.
- The second part of this chapter studies initiatives from other international (e.g., ITU-T) and European (e.g., CEN) standards bodies. For instance, the working-groups and expected deliverables from ITU-T's Focus Group DLT are analyzed in detail.

  The above two parts of this chapter provide an overview of various standardization initiatives specific to blockchain and DLT, and showcase standardization perspective of the topics discussed in Chapters 1, 2 and 4.
- The final part of this chapter reviews standardization initiatives concerning blockchain, digital trust and Smart ICT topics. This part provides insights on standardization developments related to the topics in Chapter 3 and the last part of Chapter 2.

1

Blockchain – A conceptual overview

1. Blockchain – A conceptual overview

The ever-increasing interconnectedness and integration in today's society have resulted in business networks wherein economic activity transcends national, geographic, and jurisdictional boundaries. Such business networks typically enable marketplaces where stakeholders such as producers, consumers, distributors, intermediaries and partners trade on objects of value, known as assets. In this context, an **asset** could be tangible and physical (e.g., mobile phones, real estate) or intangible and virtual (e.g., data, bond certificates, patents) and a **transaction** may comprise asset ownership, transfer, or other activities that create value in the business network. Details about trade transactions (e.g., products, costs, history of account balance) are recorded using **ledgers** to keep track of asset ownership and transfers [3]. In situations where a business participates in different types of economic activities, a common practice consists in maintaining multiple ledgers, each corresponding to an individual economic activity.

The current practice of creating and maintaining business ledgers relies heavily on centralized, trust-based, third-party systems. As a result, in some scenarios, current business ledgers become inefficient, expensive, non-transparent, and vulnerable to fraud and misuse [6]. For instance, the centralized nature of the current system, along with trust requirements, result in bottlenecks and slowdown of transactions settlement. Similarly, the lack of transparency and susceptibility to fraud lead to disputes that are costly to resolve (e.g., by reversing various transactions). Finally, since each participant in the business network is responsible to maintain its own ledger, out-of-sync copies become a reality and lead to faulty or delayed decision-making, which further results in missed business opportunities.

The blockchain technology has the potential to address the limitations of current business ledgers and be a disruptive force in transforming the way businesses are organized. In contrast to traditional ledgers, a **blockchain** is a **distributed** and **shared** digital **ledger** that records all transactions that take place in a business network. The business network is typically represented as public or private peer-to-peer network depending on the business context and the ledger is **decentralized** in the sense that the blockchain database structure is replicated across many participants/nodes in the network, each of whom collaborate in its maintenance [6]. To ensure that ledger transactions are synchronized i.e., only validated transactions are written in the blockchain and are written in the same order across all replicas, a blockchain network uses **consensus** mechanisms [7].

The information in a blockchain is recorded as blocks where a new transaction is linked/**chained** to previous blocks in an append-only manner using cryptographic techniques which ensure that a transaction cannot be modified once it has been written to the ledger. Because of this **immutability** property, blockchain is sometimes defined as a system of records that simplifies the task of determining the provenance of information. State-of-the-art blockchain solutions use **smart contracts** to support consistent update of information, to enable ledger functions (e.g., querying), and to automate aspects of transactions management (e.g., automatic calculation of account balance, controlling access to information)[1].

In the rest of this chapter, a detailed description of the basic concepts of the blockchain technology, including its working and novel characteristics, are provided.

[1] Given that this is a rather new paradigm, the **ISO/TC 307** Blockchain and Distributed Ledger Technologies is working towards standardization of its **taxonomy** and **ontology** as well as to provide a **reference architecture** through its working-group **WG 1**.

1.1 How blockchain works

A block consists of a set of transactions that are grouped together to improve logical organization and scalability. In general, a block includes a standard set of attributes that are necessary for its functioning such as a block header, a hash pointer to previous blocks, timestamp, nonce, transaction counter and the set of transactions. However, the specific structure, attributes and the number of transactions within a block, as well as the design and type of blockchain varies depending on the application scenario (see Section 1.4). An overview of the general process for generating blockchain (i.e., how blockchain works) is given below.

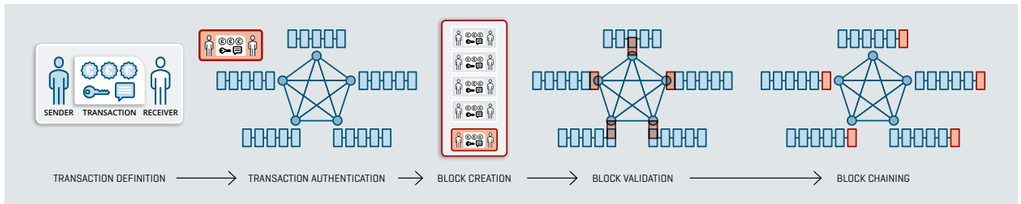


Figure 1: Process of creating and validating transactions in a blockchain

The first block called the genesis block is hardcoded at the start of the blockchain and all subsequent blocks are chained (i.e., have a reference) to the previous blocks, justifying the name blockchain. Figure 1 illustrates the general process of creating and validating transactions in a blockchain [1] [8]. The steps involved in the process are:

1. **Transaction definition:** Consider that two nodes in the blockchain network agree on a transaction. The first node Sender then creates a transaction and sends it to the network. For instance, the transaction message could include information such as the cryptographic public address of Receiver, transaction details (e.g., amount to transfer, reference to previous transactions), and a cryptographic digital signature of Sender that proves the authenticity of the transaction.
2. **Transaction authentication:** The nodes in the network receive the transaction message and validate the authenticity of the message by verifying the digital signature. The authenticated transaction is placed in a pool of pending transactions [1].
3. **Block creation:** One of the nodes in the network encapsulates pending transactions in a block and alerts the nodes across the network about the newly built block for its validation.
4. **Block validation:** The validator nodes in the network receive the new block and work to validate it through an iterative process that requires consensus from a majority of nodes in the network. These validator nodes are often referred as **Miners** [1].

   Different validation techniques are used by different blockchain platforms. For example, bitcoin uses Proof-of-Work [9] [10], Ethereum Metropolis uses a variant of Proof-of-Stake [11] [12] and Ripple builds on the Byzantine fault tolerance protocol [13]. The primary goal of these techniques is to ensure that every transaction is valid and synchronized and that fraudulent transactions remain impossible.

   In general, the miner who first resolves the computation publishes the results to the entire network. At this point, the transaction is considered as confirmed.
5. **Block chaining:** Once all transactions are validated, the new block is chained with the previously validated blocks, **forming the blockchain**. The current state of the ledger is then broadcasted to the network.

Note that the process of validation can also be performed at the level of transactions instead of a block (differing from Step 3 above). In this case, miners validate individual transactions (Step 4) and validated transactions are grouped as blocks (along with Step 5) eventually.

1.2 Network model

Decentralization is one of the core benefits and services provided by the blockchain technology. A typical blockchain network, as the one supporting bitcoin, is structured as a peer-to-peer (P2P) network on top of the Internet [3] [14]. P2P means that the computers participating in the network are all equal peers and that they all provide network services. The network topology is flat in the sense that nodes interconnect in a mesh structure, with no centralized service or hierarchy, and reciprocity acting as the incentive for participation. Such P2P networks are inherently resilient, decentralized, and open, precisely reflecting the core characteristic of the blockchain technology.

Nodes in a blockchain network, though equal, may take different roles depending on the functionality they are supporting [3]. For instance, a node could take one or more of the following roles:

- **Routing**: Each node in the network includes the routing function (receiving and forwarding messages) since it maintains connections with peers, and validates and propagates transactions/blocks.
- **Maintaining blockchain database**: Some nodes maintain a replica of the blockchain/shared ledger and autonomously and authoritatively verify transactions.
- **Mining**: A set of nodes serve as miners by participating in the process of creating new blocks (e.g., by running mining algorithms such as Proof-of-Work, as discussed in Section 1.5). In addition to mining and routing, these nodes could also maintain a replica of the blockchain.
- **Application-specific functions**: Some nodes in the network specialize in running application-specific functions such as certain smart contracts features or digital wallets. Similarly to the mining nodes, this category of nodes could maintain a blockchain replica and/or participate in the mining process, in addition to routing and running application-specific functions.
- Finally, there could be complementary nodes running other specialized blockchain protocols in the network.

Figure 2 illustrates the typical nature of centralized, distributed and decentralized systems, based on the seminal work in [15]. In a centralized system, a single node controls and manages the entire system while all other entities depend on its services (e.g., a typical client-server paradigm). A distributed system in contrast spreads the tasks of data storage and computation across multiple nodes, providing economies of scale and fault tolerance. However, a central process governs the system and controls the storage and computing nodes.

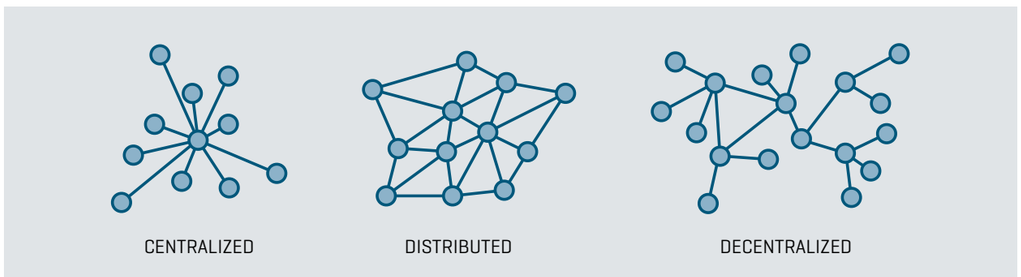


Figure 2: Different types of networked systems

In a decentralized system, control over network entities is distributed among multiple nodes, removing the system's dependence on a single process for governance, while ensuring high levels of fault tolerance and scalability. The basis for decentralizing control in blockchain consists in distributing the right to create, authenticate and verify the blocks fairly among the nodes in the network (i.e., to distribute various roles among the network nodes fairly and to employ efficient consensus mechanisms). It is important to note that the blockchain technology is not designed standalone and requires various other technologies as supporting underlying infrastructure. For example, blockchain needs Public Key Infrastructure by design (see Chapter 3), and services such as BigChainDB and IPFS to store large amounts of data in a scalable and decentralized manner [16] (see Chapter 2).

1.3 Blockchain as a database structure

Blockchain is a ledger that records all the transactions in the network. This ledger is decentralized in the sense that the blockchain database structure is shared and distributed among many nodes in the network, each of whom collaborate for its maintenance. In this context, the notion of data storage and management in blockchain becomes interesting and is discussed first in this section. Then, various properties of the blockchain database structure are studied particularly from decentralization point of view. Finally, a comparison is made between the properties of traditional blockchain databases (e.g., built for bitcoin) and state-of-the-art distributed databases. This comparison provides insights on decentralized blockchain databases.

1.3.1 Data storage and management

Blockchain can be viewed as a database technology that forces every new transaction to have the output of another transaction as its input[2]. This implies that the asset referenced in a transaction is traceable through the blockchain up to the genesis block, simplifying the task of determining the provenance of information. This aspect of blockchain can be highly useful for industries in which transparency as well as auditability and traceability are desirable features. For example, blockchain could record all events concerning the lifecycle of an artwork (e.g., creation, exhibition, transfer, ownership) as transactions and establish the provenance of the artwork, which is for instance useful to know if the art is original or has been forged [17] (see Section 4.3).

When a node creates a new block, it includes in the header of this block a reference to the previous block. Data is hence stored in the blockchain in a **chronological order** in an append-only manner, making the database structure t**amper-resistant** as well as **immutable** by design. Furthermore, if another node verifies the referenced hash to be the same as it recognizes, it implicitly **verifies** that both nodes agree on the **entire history of the blockchain**. This chaining of transactions distinguishes blockchain from other distributed ledger technologies while being consensus-oriented unites them [18].

One aspect of blockchain data management that was proposed in the context of bitcoin concerns the **longest-chain rule**. For a given block on the chain, there is a single path to the genesis block. However, there can be forks while traversing the blockchain from the genesis block. Forks typically come into existence when blocks are created by multiple nodes almost at the same time. In such situations, nodes in the network build onto whichever block they receive first and the probability that the miners continue to solve blocks simultaneously on separate chains diminishes with each mined block. At a given point, the longest chain is considered as the valid one (since most effort is taken to produce it) and it overtakes other smaller chains that are consequently dropped. Since a miner gains less reward for working on a shorter chain, miners have an incentive to reach consensus rapidly and to work on the mutual version of the blockchain (see Proof-of-Work in Section 1.5 for more details).

[2] Bitcoin implements this by means of *unspent transaction outputs* (UTXO) model where bitcoin cryptocurrency is linked to public keys of users and UTXO provides transactions in which bitcoins were received by the user but not spent yet [5].

1.3.2 Blockchain database structure and decentralization

The true potential of blockchain can be realized within a decentralized network where the data in the blockchain is shared and replicated across many nodes. Each node then has the possibility of verifying the actions of other nodes in the network, as well as the ability to create, authenticate and verify the new data to be recorded on the blockchain. This is true particularly for public and permissionless blockchains (see Section 1.4).

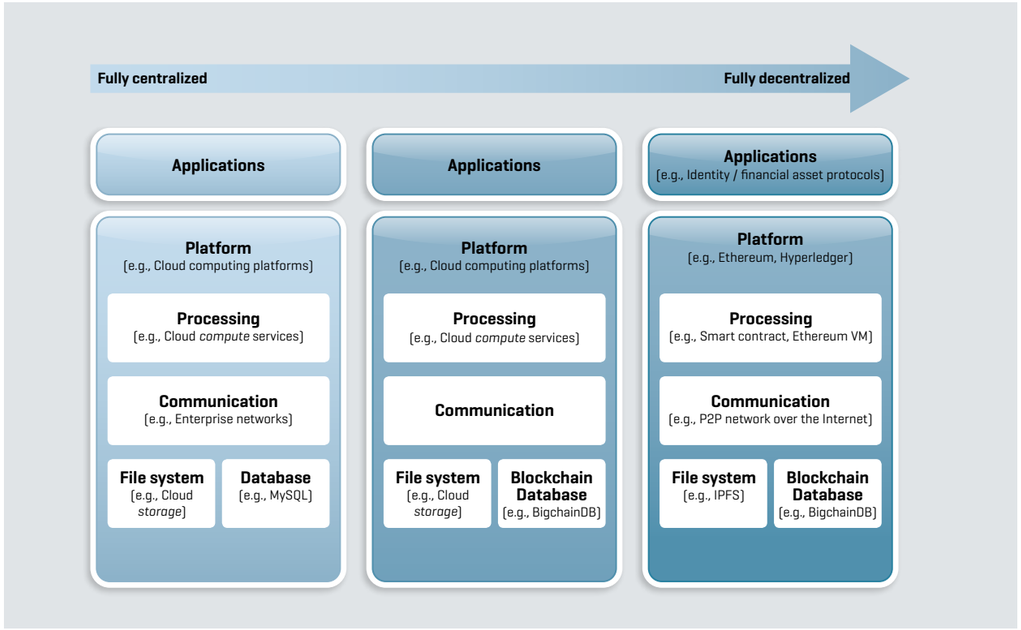


Figure 3: From traditional centralized cloud computing ecosystem (left) to fully decentralized blockchain ecosystem (right) [16]

Based on [16], Figure 3 clarifies how a blockchain database structure is associated with other communication and processing technologies, and compares its usefulness with respect to various decentralization settings (fully centralized, partially decentralized and fully decentralized contexts). The blockchain database structure is complementary to decentralized smart contracts processing, file system and communications building blocks [19]. It can be encapsulated with decentralized computing platforms (e.g., Ethereum), and be used for a wide range of applications such as identity protocols [20], financial assets protocols [5] [3] and glue protocols [21].

A blockchain database structure can also work in completely centralized or partially decentralized paradigms. For example, the former is possible in scenarios where decentralizing only storage brings benefits. The latter can be used when scalability needs are greater than the capabilities of existing decentralized processing technologies. In this case, blockchain provides a bridge to eventually be a fully decentralized system.

1.3.3 Comparing attributes of traditional blockchain, distributed and decentralized databases

Modern distributed databases have storage capacities in the orders of petabyte and beyond, throughput exceeding a million transactions per second, while maintaining the latency within a fraction of a second. Their design ensures that throughput and capacity increases as the number of nodes in the system increase. A number of additional features enable querying, insertion and access control over data, based on rich set of languages such as SQL and NoSQL [16]. In contrast to distributed databases, bitcoin blockchain for example, has a capacity in the orders of gigabytes, throughput of seconds for a few transaction and the latency of minutes before a single write. The performance of the system decreases when the number of nodes increase. It is estimated that the network traffic quadruples when the number of nodes double, with no improvement in throughput, latency or storage capacity. Moreover, languages for data management are limited.

	Distributed databases	Traditional blockchain	Decentralized databases (desired for blockchain)
Throughput (that increases with the number of nodes)	High	Low	High
Latency	Low	High	Low
Capacity (that increases with the number of nodes)	High	Low	High
Querying features	Rich	Limited	Rich
Access control capabilities	High	Limited	High
Decentralized control	Not possible	Possible	Possible
Immutability	No	Yes	Yes
Creation & transfer of assets	Not possible	Possible	Possible

Table 1: Comparison between traditional blockchain and distributed databases; derivation of desired properties for decentralized blockchain databases [16]

To meet the full potential of the blockchain technology, as outlined in Table 1, the underlying decentralized databases need to combine the key benefits of both abovementioned databases, and output high throughput, capacity, scalability, low latency, and a rich set of query languages [16]. Blockchain and decentralized database solutions that are currently available in the market are discussed in Chapter 2.

1.4 Permissioned and permissionless blockchains

One primary decision that needs to be made when using a blockchain concerns with its scope (e.g., whether to use a public or a private blockchain). This decision depends on the application scenario and parameters such as the access control requirements, regulatory compliance goals, and entities that are entitled to be miners.

A classification of blockchain permissions and scope is as follows [22] [18]:

- **Public blockchain:** The blockchain in which there is no restriction on reading data and submitting transactions for inclusion into the blockchain.
- **Private blockchain:** A blockchain that allows direct access to data and transactions submission only to a predefined list of entities.
- **Permissionless blockchain:** The blockchain in which there are no restrictions on identities of transaction processors.
- **Permissioned blockchain:** A blockchain that allows transaction processing only to a predefined list of subjects with known identities.

There is a spectrum of possibilities among these configurations. For example, a permissioned blockchain could be either private or public. Blockchain that uses policies to constrain network participation as well as access to records are both **permissioned and private**. These are particularly useful for banks and financial institutions that want to leverage the potential of blockchain while maintaining fine-grained control over data access and transparency. In contrast, blockchain that gives permissions to read data and to submit transactions to anyone (or to a list of collaborating institutions), but controlled only by pre-authorized nodes, are **permissioned and public**. Similarly, blockchains that are not only open for any participant to join as users and serve as nodes but also for the data to be publicly transparent are **permissionless and public**. This model is generally adopted by cryptocurrencies such as bitcoin. Table 2 compares private permissioned and public permissionless blockchain.

	Permissioned blockchain (Private)	Permissionless blockchain (Public)
Access granted	Authorized to a pre-defined list of users	Open access
Approach to traditional business processes and regulations	Aims to follow standard business processes and regulations such as KYC (Know Your Customer), HIPAA (Health Insurance Portability and Accountability Act) and GDPR (EU General Data Protection Regulation)	Aims to create censorship resistant, anonymous transactions, ideally outside the current legal framework
Miners (validators)	Pre-selected, trusted miners	Anonymous, fully decentralized miners
Typical application domain	Enterprise-level systems	Permissionless innovation, open-access applications

Table 2: Comparison of private permissioned and public permissionless blockchain

Note that using a public blockchain results in better transparency and auditability but has a complex performance and cost model. Private blockchain, on the other hand, is the most flexible for configuration since it is governed and hosted by a single organization but has limitations with respect to public blockchain properties such as equal rights, transparency and auditability [1] [23].

Similarly, permissioned blockchains allow recording larger amount of transaction details, and allow specifying fine-grained policies wherein some participants may view only abstract information while others, such as auditors, have access to broader range of transactions. For example, if Party A transfers an asset to Party B, both parties can see the details of the transactions. An external Party C can know about the existence of this transaction but not its details. For an auditor or a regulator, full details of transactions can be made available. Such granular permissions management may not be feasible in case of permissionless blockchain. On the contrary, certain design choices made in permissionless blockchain become non-essential for scenarios using permissioned blockchain. For example, Proof-of-Work is suitable for bitcoin (permissionless blockchain) to counter Sybil attacks[3]; but, in case of permissioned blockchain, since the identity of each node is known, Sybil resistance becomes superfluous and a more cost-effective alternative such as a threshold signature scheme suffices [18]. Chapter 3 discusses such security and privacy issues in detail.

Based on the discussions in [23], Table 3 summarizes the relationship between blockchain permissions, their deployment model (with varying degrees of decentralization), and its impact on: i) blockchain features (e.g., immutability, trust, transparency), ii) cost, iii) performance and iv) safety. Permissioned blockchain is designed to be less decentralized than permissionless blockchains but significantly more decentralized than typical master-access databases. Therefore, there are often trade-offs between permissioned and permissionless blockchains including transaction processing, rate, cost, censorship-resistance, reversibility and flexibility in changing and optimizing the network rules [24].

Configuration	Blockchain design choices	Blockchain features	Cost efficiency	Performance	#Failure points[4]
		Favorability/impact			
Fully centralized	Application offered by a single provider (e.g., government)	Low	High	High	1
	Application offered by alternative providers (e.g., banks, online payments)				
Partially centralized & partially decentralized	Permissioned blockchain with fine-grained control over operations (e.g., at the transactions level)	Medium	Medium	Medium	All
	Permissioned blockchain with permissioned miners (write) but permissionless normal nodes (read)				
Fully decentralized	Permissionless blockchain	High	Low	Low	Majority (nodes, power, stake)

Table 3: Blockchain design choices related to (de)centralization and the impact of each choice on the favourability of various properties [23]

[3] Sybil attacks on a blockchain network can allow a single user to generate several online identities to influence and manipulate the consensus process [166].

[4] The number of failure points concerns the safety/fault tolerance of blockchain. For instance, in a fully centralized configuration, the failure of the "central" node alone results in the failure of the entire system.

1.5 Consensus methods

The blockchain technology enables participants to read from and update to a shared ledger (blockchain) whose state is maintained collectively by the network in a decentralized manner [2]. To maintain the state of the blockchain, typically a consensus mechanism is used which guarantees integrity and consistency, and ensures a common, unambiguous ordering of transactions and blocks. In other words, consensus protocols maintain the sanctity of data recorded on the blockchain and provide the building blocks that allows a blockchain platform to function correctly in normal as well as adversarial conditions [25] [26].

Permissionless blockchains expect to have a large number of anonymous and untrusted participants because any node can join the network, requiring consensus mechanisms to take into account inherent maliciousness (e.g., resistance against Sybil attacks). For example, bitcoin solves this problem by designing a consensus protocol where the nodes are obliged to prove that they have expended certain amount of energy. This protocol is widely known as the Proof-of-Work (PoW). Different techniques are used by different permissionless blockchain platforms (e.g., bitcoin uses Proof-of-Work while Ethereum Metropolis uses a variant of Proof-of-Stake) and are discussed further in this section.

In a permissioned blockchain, the nodes are semi-trusted since only verified and registered members take part as participants. The number of nodes are expected to be small, allowing one to employ consensus mechanisms other than the PoW [2]. Many aspects of existing research in the field of Byzantine Fault Tolerance (BFT) in distributed systems are also applicable in the context of reaching consensus in permissioned blockchains. Consequently, existing blockchain platforms (e.g., Hyperledger [27]) have used well-known Practical Byzantine Fault Tolerance (PBFT) algorithm [28] and its variant such as SIEVE and Cross-Fault Tolerance (XFT) [29] to ensure consistent ordering of transactions and to handle non-determinism in smart contract (see Section 1.6) execution. The rest of this section also discusses this class of consensus mechanisms.

1.5.1 Proof-of-Work (PoW)

Proof-of-Work is a piece of data that is: i) difficult (costly, time-consuming) to produce, ii) easy for others to verify, and iii) satisfies certain pre-defined conditions [9] [10]. In general, the task of generating PoW is designed to be a random process with low probability of success in order to ensure that a lot of trial and error happens on average before producing a valid PoW.

Bitcoin for instance uses a variant of PoW called HashCash for block validation and chaining [5]. As discussed in Section 1.1, when a transaction/block is pending, network participants work to validate it through an iterative process that requires consensus from a majority of nodes. In case of bitcoin, to validate a transaction/block, miners compete to generate a PoW such that the new block hashes to a value satisfying the current pre-defined target (as illustrated in the example below). This process ensures that each **block** is **generated** only after **certain amount of work** has been done. Moreover, due to the low probability of success in generating target PoW, it is unpredictably as to which node in network will be able to generate the next block.

Example: For the sake of clarity, consider the following example illustrated in [10]. Let the base string be "Hello, world!" and the target be a variation of the string that SHA-256 hashes to a value beginning with "000". To find the target string, nodes competing through PoW vary the string by appending an integer value called a nonce and increment it in each iteration. In this case, the target variation of "Hello, world!" is achieved after 4251 tries with first four digits as zeros [10].

- "Hello, world!0": 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
- "Hello, world!1": e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
- and so on ...
- "Hello, world!4249": c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
- "Hello, world!4250": 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

Generating 4251 number of hashes is not a large amount of work for modern computers. It is only used as an example PoW here. In practice, bitcoin varies the difficulty and the amount of work required to generate a block to keep a roughly constant rate of block generation. Currently, the difficulty of this work is set in the bitcoin network to limit the rate at which new blocks can be generated to one in every ten minutes.

The miner who first resolves the PoW by finding the target, publishes the results to the entire network. All other nodes can easily verify the result and consequently agree on block validity and new state of the blockchain. The successful miner is rewarded and new bitcoins (cryptocurrency) are generated in the system. Hence, Proof-of-Work mining accomplishes several tasks [18]:

- It allows anyone with a processing unit to participate in the process of creating new blocks.
- It validates the legitimacy of a transaction.
- It allows the network to reach consensus and in the process of doing so, avoids issues such as double spending and Sybil attacks.
- It introduces new cryptocurrency (e.g., bitcoin) into the system at a steady rate and rewards miners using an arguably fair distribution mechanism.
- It makes blocks tamper-resistant. Each block contains the hash of the preceding block, and therefore, each block is associated with a chain of blocks that together comprise a very large amount of work. Any changes to a block requires regenerating all successors and redoing all work they contain, making the blockchain tamper-resistant.

While the PoW model supports open-ended participation, some research argues that its application is hindered for scenarios that need immediate transaction finality and have high transaction rates (e.g., much greater than a block per ten minutes). Similarly, the amount of power consumption due to PoW is very high. For example, [30] suggests that the amount of electricity wasted in bitcoin mining is comparable to the average electricity consumption of Ireland. On the other hand, consensus models designed for permissioned systems do not scale beyond tens of peering nodes and cannot have any open-ended participation. The task of designing new consensus models to address the abovementioned limitations is increasingly emerging as an active research area [2] [26]. Other consensus mechanisms that are gaining industry and academia attention are discussed below. The platforms using each of these mechanisms are outlined in Chapter 2.

1.5.2 Proof-of-Stake (PoS)

The purpose of Proof-of-Stake is same as that of Proof-of-Work but the process to achieve the goal is different. In contrast to PoW where miners solve complex cryptographic challenges to validate transactions and to create new blocks, in PoS the creator of the next new block is chosen in a deterministic (pseudo-random) way, based on its wealth, which is defined as the **stake**. The stake in this case typically refers to the possession of tokens in the system (e.g., cryptocurrency).

The basis for decentralizing control in blockchain is for the network to distribute the right to create blocks fairly among the nodes. If the creator of blocks is selected purely based on the possession of tokens, the richest member in the network will have an asymmetric advantage, resulting in undesirable centralization. To address this challenge, several methods for node selection have been proposed:

- One approach consists in looking for the lowest hash value in combination with the size of the stake [31] [32]. This introduces a degree of randomization in selecting the next block creator. Moreover, in public blockchains where all participants know the stakes of all members, each node can predict which node will have the right to create/forge [5] the next block with reasonable probability.
- Another approach combines ownership of stake and the period of time over which the tokens are held. Older and larger sets of stakes have higher probability of forging the next block. Once a stake has been used, the period of ownership is reset.

In the basic version of PoS, all tokens are usually created in the beginning and the number of tokens do not change over time, unlike in a system using PoW. Consequently, there are no block rewards (e.g., as in bitcoin) and the forgers take only the transaction fees. In this context, a PoS system has the potential to result in lower equilibrium transaction fees [26] and lower long-run operational fees could improve competitiveness as well as alternative cost-efficient solutions (e.g., as compared to bitcoin). Due to significant reduction in the scale of resources required, transaction fees could also be reduced even further.

In situations where the stake is escrowed for creating a block of malicious transactions, the network rejects the transaction and forfeits the escrowed stake. Thus, a PoS system can provide increased protection from malicious behavior in the network because [2]: i) executing an attack would be highly expensive since attackers need to gain more than half of the stake in the network to be able to maintain the longest chain and manipulate the blockchain and ii) the incentives from an attack are diminished. This model is designed to ensure that attackers could suffer severely from their own attacks.

One limitation of PoS that has been highlighted in the literature [33] is described as the "nothing at stake" problem. In the case of a consensus failure, block-generators have nothing to lose by voting for multiple blockchain-histories, preventing the consensus from ever resolving. Since the cost of working on several chains is minimal (unlike in the PoW systems), anyone can abuse this problem and attempt to double-spend "for free".

1.5.3 Byzantine fault tolerance

Many problems studied in the field of Byzantine Fault Tolerance (BFT) are applicable in case of blockchains particularly for reaching consensus, replicating state, and broadcasting transactions in situations where the network is not trustworthy (e.g., because of crash failures, uncertain connectivity, or system compromise by an adversary). Consequently, a number of solutions in the literature have proposed the use of BFT – and its variants – in permissioned and private blockchains. The most prominent of such solutions are based on the well-known Practical Byzantine Fault Tolerance (PBFT) algorithm [28] and its variant called SIEVE. The use of these algorithms in blockchain ensures consistent ordering of transactions in the ledger across all replicas and allows handling of non-determinism in smart contract (see Section 1.6) execution.

Practical Byzantine Fault Tolerance (PBFT): The PBFT algorithm proposed by Castro and Liskov [28] was one of the seminal solutions for achieving consensus in the presence of Byzantine failures [6]. It uses the concept of replicated state machine and a voting mechanism among replicas for consistent state changes. Compared to existing solutions, this algorithm optimizes several aspects for the system to be practical such as: i) the process of signing and encryption of messages exchanged between replicas and clients, ii) reducing the size and number of messages exchanged etc. This algorithm can tolerate f byzantine failures with the help of 3f+1 replicas, imposing low overhead on performance. In practice, however, this algorithm scales only up to 20 replicas since messaging overhead increases significantly as the number of replicas increase.

[5] In some cryptocurrency solutions that use PoS, the blocks are said to be **forged** rather than **mined**.

[6] Byzantine failures are defined as arbitrary deviations of a process from its assumed behavior. Such failures include software bugs, transient and permanent malfunction of system components, or malicious attacks.

SIEVE: Non-determinism in smart contracts might produce different outputs when executed by different replicas in a distributed network. SIEVE handles transactions that are usually deterministic but sometimes yield different outputs [2]. This protocol treats a smart contract as a black box; it executes all operations speculatively and then compares the outputs across replicas. If the protocol detects a minor divergence among a small number of replicas, the diverging values are filtered. If the divergence occurs across several processes, then the operation itself is filtered [2].

Cross-Fault Tolerance (XFT): BFT protocols assume a powerful adversary with ability to control compromised nodes as well as the message delivery of the entire network. This assumption induces complexity in BFT protocols and makes them less efficient [2]. The cross-fault tolerance (XFT) approach instead assumes that the adversary cannot control majority of the nodes and generate network partitions at will at the same time [29]. This simplified model is particularly interesting in blockchain where the nodes might have financial incentives to act maliciously, yet lack the means and capabilities to compromise communications between nodes or create arbitrary network partitions [2]. XFT provides correct service as long as majority of the replicas are correct and can communicate with each other synchronously. It uses same number of resources as protocols that can tolerate simple crash failures yet tolerate Byzantine faults.

1.5.4 Proof-of-Elapsed-Time (PoET) and Federated Byzantine Agreement (FBA)

This section reviews some other consensus mechanisms that fall between the extremes of BFT protocols (used in permissioned blockchains) and Proof-of-Work (used in permissionless blockchains), based on [2].

Proof-of-Elapsed Time (PoET): PoET is based on the notion of leader election and requires all miners in the network to run a Trusted Execution Environment (TEE) [2] [21]. Each miner requests a wait time from the code running inside the TEE and the miner with the shortest wait time wins the lottery to become the leader. The functions within the TEE ensure that their execution cannot be tampered by external software. When a miner claims to be a leader and mines a block, it can also demonstrate the proof generated within the TEE, which other nodes can verify. For example, the leader has to prove that it had the shortest wait time and it waited for a protocol designated amount of time before starting to mine the next block. The randomness in generating waiting times ensures that the leader election is randomly distributed among all validating nodes/miners [2]. The principle drawback of this algorithm is that it is dependent on specialized hardware.

Federated Byzantine Agreement (FBA): This family of protocols depart from the traditional security assumption for consensus protocols (e.g., in BFT) by relaxing trust assumptions. For example, instead of making global assumptions about node collusions that the protocol tolerates, nodes in the network declare upfront a list of nodes that it trusts, operating somewhat in a permissioned fashion [26]. This type of consensus is used by two well-known blockchain platforms that operate global payment networks: Ripple [13] and Stellar [34].

In the Ripple consensus protocol algorithm, each node in the network maintains a *unique node list* (UNL), which consists of the identities of other nodes that are trusted not to collude against it [2] [26] [13]. Consensus in the network is achieved in multiple rounds where, in each round, all the nodes collect transactions in a data structure called the candidate set and broadcasts it to other nodes in its UNL. Each node validates the transactions, votes on them, and broadcasts its votes. The candidate set in each node is refined based on the accumulated votes and the transactions that receive the largest number of votes are passed to the next round. If a candidate set receives 80% of votes from all nodes in the UNL, the candidate set becomes a valid block and is added to the blockchain by each node. Next round of consensus is started with newer transactions and pending transactions that are not validated in the previous round of consensus [2]. The entire network reaches consensus when each individual sub-network reaches consensus.

The Stellar consensus protocol [34] is similar to the Ripple consensus protocol and FBA. In Stellar, only validator nodes participate in the consensus protocol and, similarly to Ripple UNL, each validator declares its own convincing set called a quorum slice. A quorum is a set of nodes that is sufficient to reach an agreement and a quorum slice is a subset of a quorum that can convince one particular node about agreement [2]. A quorum slice from each validator must sufficiently overlap with the convincing-sets of other nodes for preventing forks. A node accepts a transaction for the ledger when a threshold of nodes in its convincing set confirms it [26]. To allow open participation, Stellar exploits the notion that an individual node can appear on multiple quorum slices, allowing the nodes to choose a set of nodes within its slice.

Based on the survey in [2] and discussions in this section, Table 4 provides a comparative analysis of popular consensus schemes across a range of blockchain parameters.

	PoW	PoS	PoET	BFT and its variants	FBA
Blockchain type	Permissionless	Both	Both	Permissioned	Permissionless
Transaction finality	Probabilistic	Probabilistic	Probabilistic	Immediate	Immediate
Transaction rate	Low	High	Medium	High	High
Need for tokens	Yes	Yes	No	No	No
Cost of participation	Yes	Yes	No	No	No
Scalability of peer network	High	High	High	Low	High
Trust model	Untrusted	Untrusted	Untrusted	Semi-trusted	Semi-trusted

Table 4: Analysis of consensus models across several blockchain parameters [2]

1.6 Smart contracts

The notion of a smart contract was originally defined as a standalone topic and did not require a blockchain to run. However, the advent of blockchain has resulted in a significant increase in market attention on smart contracts, and the state-of-the-art has so far indicated several benefits of combining the two [7]. This section first introduces smart contracts briefly and then studies their application in blockchain in detail.

1.6.1 Introduction to smart contracts

Smart contract was introduced as *a computerized transaction protocol that executes the terms of a contract* [35]. According to this seminal work, the goal of a smart contract in terms of its functionality is threefold. First, to satisfy general contractual conditions such as payment terms, confidentiality and enforcement. Second, to minimize malicious and accidental exceptions, and third, to reduce the need for trusted intermediaries. Similarly, in terms of economic benefits, the goal of a smart contract is to reduce the losses due to frauds and arbitrations as well as to lower the costs of enforcement and transactions management.

The definition in [35] has been adapted over time in many contexts. For example, [36] defines a smart contract as a *secure and unstoppable computer program representing an agreement that is automatically executable and enforcable*. This definition underscores that smart contracts execute automatically when certain pre-defined conditions are satisfied, and they are enforceable in the sense that all contractual terms execute as defined and expected, even in the presence of adversaries. A further refinement of this definition highlights that smart contract enforcement must work on the principle of code is law, meaning that there is no need for an arbitrator or a third party to control or influence the execution of the smart contract. This implies that a smart contract must be fault tolerant, be executable in reasonable amount of time, and support decentralized execution.

A limitation of the above definition is that smart contracts cannot access external data that might be required to control the execution of the business logic. To deliver data from external sources (e.g., IoT devices, stock market feeds) to smart contracts, the notion of **Oracle** was introduced and the above definition was refined to suggest that smart contracts need not be automatically executable, instead be automatable [37]. Given the confluence of fundamental properties, the above set of definitions by themselves indicate why execution of smart contracts on blockchain platforms is a natural and mutually beneficial phenomenon.

1.6.2 Smart contracts and blockchains

The first-generation blockchain (sometimes defined as **blockchain 1.0**) which realized bitcoin/cryptocurrency partially adopted and implemented the notion of a smart contract to regulate transactions and transfer of value (e.g., bitcoin) in a peer-to-peer network [5]. However, the capability to support programmable transactions and auxiliary data (e.g., representing digital or physical assets) was highly limited. The second-generation blockchain **(blockchain 2.0)**, which is ubiquitous today, provides a general-purpose programmable infrastructure wherein records can be maintained in public or private ledgers. In this context, smart contracts are programs that can express complex transactions with triggers, conditions and business logic. They can support consistent update of information and enable ledger functions as well as automate various aspects of transactions. In support of these developments, a number of programming languages to encode smart contracts such as [38] are now available. Several use cases and the role of smart contracts in state-of-the-art blockchain platforms such as Ethereum and Hyperledger are discussed in Chapter 2.

[7] The ISO/TC 307 on Blockchain and Distributed Ledger Technologies has created a working-group WG 3 Smart contracts and their applications, which is carrying out techno-legal standardization activities (see Chapter 5).

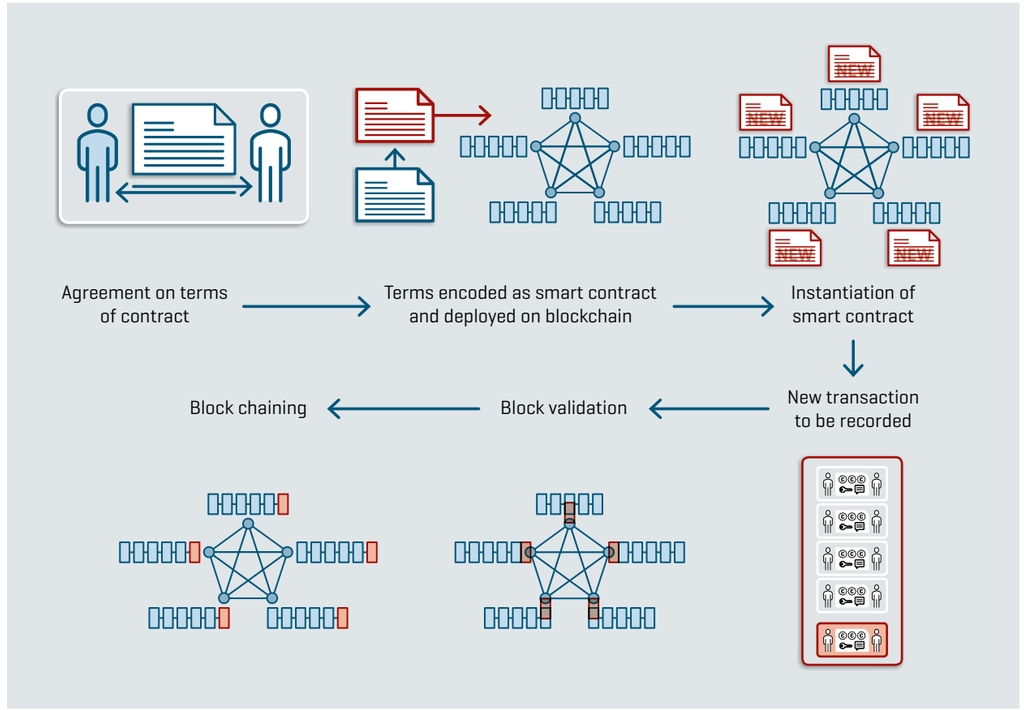


Figure 4: Process of running a smart contract on blockchain

Figure 4 outlines the steps involved in running a simple smart contract on a blockchain (based on [8]) and is described below:

1. Consider that two parties agree on the terms of a contract.
2. Based on the agreed terms, the conditions for smart contract are established. These conditions as well as relevant actions are encoded within a smart contract (e.g., using programming languages such as Solidity [38]) and deployed on a blockchain (e.g., on Ethereum platform [19] [39]).
3. An instance of the smart contract is created in order to initiate new system processes and to run the first transaction.
4. Each time conditions in the smart contract are satisfied (e.g., availability of sufficient amount), a set of actions (e.g., transfer amount) are triggered and encapsulated as transactions/blocks to be recorded in the blockchain.
5. When miners validate the transaction/block, it is recorded to the blockchain as an entry in the immutable shared ledger.

Gaining consensuses is one of the major features on which blockchain relies. In this context, correct functioning of consensus protocols require smart contracts to be deterministic in at least two ways (see Section 1.5 within the context of Byzantine fault tolerance). First, irrespective of the node on which the smart contract is executed, it must provide same results. The paradigm of distributed consensus might fail if nodes output even slightly different results. Second, the language in which smart contracts are written must ensure that its functions provide consistent output independently to the invocation process. For instance, smart contracts should be unlike some scripting languages that can produce different results on different web browsers since it may lead into bugs and loss of integrity and stability during contracts enforcement. Chapter 3 discusses digital trust aspects of smart contracts in detail.

2

Blockchain technology landscape analysis

2. Blockchain technology landscape analysis

The previous chapter described fundamentals of blockchain starting from a conceptual overview on how blockchain works, to network and data management models, and finally to consensus methods and the role of smart contracts. This chapter builds on these concepts and provides an overall analysis of the technology. First, an analysis of blockchain platforms is provided, then insights on various consortia that were formed by companies, research institutions, and governments to realize their blockchain strategy are outlined, and finally, the relationship between blockchain and Smart ICT (Cloud computing, Internet of Things and Big data) is established to understand blockchain from a global ICT ecosystem point of view.

2.1 High-level analysis of blockchain platforms

A number of open-source platforms that allow users to create their own blockchain applications have been developed. Table 5 lists such platforms and characterizes their properties ranging from capabilities to target application domains, scope and techniques used, based on [40]. Note that, given increased research and industry attention in this area, the list of platforms in the table is not exhaustive.

One category of platforms build on the blockchain technology for cryptocurrencies to accommodate the notion of **digital assets**. In contrast to cryptocurrencies that are created and derive their values from blockchains, digital assets are a generalization in the sense that they are issued by real world entities and their existence/exchanges are recorded by blockchain. For instance, Multichain and Corda are two blockchain platforms that use the **transaction-based data model** of bitcoin but allow storage and tracking of digital assets history. Differently from bitcoin, these platforms target private settings that allow enterprises to form closed networks and trade/control assets.

Another category of platforms goes beyond creation and management of digital assets and supports **general user-defined application**s, largely via smart contracts. The most popular of such platforms is Ethereum. It adopts an **account-based data model** and supports public permissionless applications ranging from simple crowdfunding campaigns to complex investment funds like The DAO (Decentralized Autonomous Organization). Monax, Hydrachain, Quorum, Dfinity and Parity are all derived from Ethereum and aim at deploying/executing arbitrary business logic on distributed shared ledgers. Quorum, for instance, is an Ethereum-based distributed ledger protocol that provides the financial services industry with a permissioned implementation of Ethereum supporting transaction and contract privacy.

Stellar, Ripple, Iroha and IOTA also adopt account-based data model, issue their own tokens, and provide their ledgers as a means to exchange tokens and micropayments. Among these platforms, Stellar is gaining increasing attention from various organizations globally for its fast, reliable and cost-effective payments infrastructure, while being public and permissionless. IOTA, on the other hand, is interesting since it allows zero-fee micropayments and enables a platform that is useful for exchanges among Internet of Things (IoT) devices. Iroha is inspired by the Hyperledger Fabric architecture and aims to provide a development environment where C++, web and mobile applications can be built.

Finally, Hyperledger Fabric and Sawtooth Lake represent the third category of blockchain platforms and support private as well as permissioned **enterprise-grade applications**. They utilize **key-value data model**, allowing applications to create and update key-value tuples (like in traditional databases) on the blockchain. Iroha complements Fabric and Sawtooth Lake by providing a library of reusable components in C++ that can be called from Golang and by emphasizing on mobile application development.

Blockchain platform	Application	Data model	Consensus mechanism	Ledger type (scope)	Smart contract	
					Execution	Language(s) supported
Corda	Digital assets	Transaction-based	Raft	Permissioned, private	JVM	Java, Kotlin
Multichain			Trusted validators (round robin)	Permissioned, permissionless, public, private	Native	C++
Openchain[8]			Single validator	Permissioned, private	--	--
Stellar	Digital assets	Account-based	Stellar consensus	Permissionless, public	--	--
Ripple			Ripple consensus	Permissionless, public	--	--
IOTA[9]	Digital assets (focus: IoT)	Account-based	IOTA's Tangle consensus	Permissioned, public	--	--
Ethereum	General purpose	Account-based	Homestead: PoW (Etash) Metropolis: PoS (Casper)	Permissionless, public	EVM	Solidity, Serpent, LLL
Monax			Tendermint (combination of PoS & PBFT)	Permissioned, private	EVM	Solidity, Serpent, LLL
Hydrachain[8]			Trusted validators (majority)	Permissioned, private	EVM, Python	Solidity, Serpent, LLL
Quorum			Raft (majority)	Permissioned, private	EVM	Golang
Dfinity[8]			Threshold relay	Permissionless, public	EVM	Solidity, Serpent, LLL
Parity			Trusted validators (round robin)	Permissionless, public	EVM	Solidity, Serpent, LLL
Hyperledger Fabric	General purpose	Key-value	Modular; PBFT (v0.6.0), ordering service Kafka (v1.0.0)	Permissioned, private	Dockers	Golang, Java
Sawtooth Lake			PoET	Permissioned, permissionless, public, private	Native, dockers	Python
Iroha[9]	Digital assets (focus: mobile applications)	Account-based	Sumeragi (BFT)	Permissioned, private	Dockers	C++

Table 5: Analysis of blockchain platforms [40]

[8] These platforms may not be in active development. For example, Openchain was last updated on GitHub in February 2016, at the time of writing this chapter.

[9] IOTA is a relatively new platform that has currently released Beta version with only a reference implementation. It is a non-blockchain type distributed ledger technology.
Iroha plans to release its Alpha version in September 2017.

It is clear that Hyperledger and Ethereum serve as reference blockchain platforms that: i) inspire many other developments, ii) are supported by a large number of stakeholders, and iii) represent two most successful yet contrasting types of blockchain implementations (e.g., Hyperledger Fabric is private and permissioned while Ethereum is public and permissionless). An overview of these two platforms is provided next in this chapter.

2.2 Hyperledger

Hyperledger is a global, open source collaborative effort, created to develop cross-industry blockchain technologies that can be used by businesses. It is hosted by The Linux Foundation and supported by a number industry leaders from healthcare, manufacturing, finance, banking, logistics and technology sectors. Within the Hyperledger umbrella, a range of projects including distributed ledger frameworks, smart contract engines, client libraries, graphical interfaces, utility libraries and sample applications are being promoted. These projects adopt a lifecycle process with five states: proposal, incubation, active, deprecated and end of life. Table 6 reports all Hyperledger projects and their current status [27] [41] as of September 2017.

Name	Status (as of Sep 2017)	Description
		Support (potentially)
Frameworks		
Burrow	Incubation	Permissioned Ethereum smart-contract blockchain
Fabric	Active	Distributed ledger in Golang
Indy	Incubation	Distributed ledger purpose-built for decentralized identity
Iroha	Active	Distributed ledger in C++
Sawtooth	Active	Distributed ledger in Python
Modules/Tools		
Cello	Incubation	Blockchain management
		Fabric, (Sawtooth, Iroha)
Cello Analytics	Incubation	Blockchain analytics
		Cello
Composer	Incubation	Development framework; tools for building blockchain networks
		Fabric, (Sawtooth, Iroha)
Explorer	Incubation	Blockchain Web UI
		Fabric, (Sawtooth, Iroha)
Fabric Chaintool	Active	Chaincode packaging for Fabric
		Fabric
Fabric SDK Py	Active	Fabric SDK in Python
		Fabric
Fabric SDK Go	Incubation	Fabric SDK in Golang
		Fabric

Table 6: Projects within Hyperledger umbrella

2.2.1 Hyperledger frameworks and tools

The first and the most widely recognized project within the Hyperledger umbrella is **Hyperledger Fabric**, which is a platform that allows industry or public domain to build distributed ledger solutions. Like other blockchain technologies, Fabric has a ledger, uses smart contracts, and is a system by which participants manage their transactions. However, in contrast to typical public and permissionless blockchains, Fabric supports traditional business networks in which **members know each other's identity but the transactions between them remain confidential** as in private and permissioned blockchains. It implements a **modular architecture** that provides functional choice to network designers and, by doing so, it accommodates the complexity and intricacies that exist across economic ecosystems. For instance, it allows network designers to plug-in specific algorithms for identity, consensus and encryption at will, offering high degrees of flexibility and scalability. In July 2017, Hyperledger announced production-ready Hyperleger Fabric V1.0. IBM is one of the leading contributors to this project.

Recently, two other Hyperledger projects, namely **Sawtooth** and **Iroha**, have also advanced their status from being in incubation to active blockchain frameworks. **Sawtooth** was originally designed by Intel to study scalability, security and privacy concerns prompted by original distributed ledgers. It is now a modular platform that allows organizations to build, deploy, and run distributed ledgers, and includes Proof of Elapsed Time (PoET) as its consensus mechanism, targeting large distributed validator populations with economical resource consumption. **Iroha**, on the other hand, is a business blockchain framework that can be incorporated into infrastructural projects requiring distributed ledger technology. It follows similar principles as that of Fabric and aims to provide a development environment where C++, web and mobile application developers can contribute to Hyperledger project.

Inspired by Hyperledger's strategy, which encourages re-use of common building blocks and enables rapid innovation of various distributed ledger components, many other platforms and tools are being developed within the Hyperledger umbrella (as listed below) [27]:

- **Hyperledger Burrow** provides a modular blockchain client with a permissioned smart contract interpreter, built in part to the specification of the Ethereum Virtual Machine (EVM).
- **Hyperledger Indy** is a platform that provides tools, libraries, and reusable components for providing digital identities rooted on blockchains so that they are interoperable across administrative domains, applications, and any other silo.
- **Hyperledger Cello** is a tool that aims to bring the on-demand (as-a-service) deployment model to the blockchain ecosystem.
- **Hyperledger Composer** is a collaboration tool for building blockchain business networks, accelerating the development of smart contracts and their deployment across a distributed ledger.
- **Hyperledger Explorer** is a tool that allows users to view, invoke, deploy or query blocks, transactions and associated data, network information, smart contracts and other relevant information stored in the ledger.

2.2.2 Hyperledger membership analysis

Hyperledger was announced in December 2015 by 17 organizations. Since then, this project attracted interest of various organizations from across the world, and at the time of writing (October 2017) this chapter, it has 20 premier members, 119 general members and 21 associate members. Table 7 presents an analysis of Hyperledger membership, (updated version of [42]), to provide insights on the trends and pulse of blockchain advancements.

Geographical distribution of Hyperledger members	Type of organization ('classic' or 'innovator')[10]	Industry allocation
Among 139 premier and general members: 51 are from the USA, 32 from China, 6 from Japan, and 4 from Canada. Within Europe: 9 organizations are from the UK, 3 from France, 4 from Switzerland, 2 from Germany and 1 each from Belgium, Estonia, Finland, Italy, Netherlands, Spain and Sweden. **University of Luxembourg (SnT) is an associate member.**	• 18 of the premier members and 51 general members are classic. • 2 of the premier members and 56 general members might be classified as innovators. • Other members are difficult to be classified in a straightforward manner. Among the innovators (general members), 10 are Chinese and 21 are based in the USA.	While classifying organizations per industry is difficult, the following provides a broad overview: • 52 software • 23 financial services • 14 ICT • 11 services (including consulting, legal, advertising) • 9 banking • 7 financial exchanges • 6 industrial (including aviation and automotive) • 3 healthcare • 2 other services • 1 government

Table 7: Hyperledger membership analysis [42]

2.2.3 Hyperledger architecture and workflow

All Hyperledger projects aim to provide business friendly solutions that are not only modular and extensible, but also secure, token-agnostic and interoperable. Moreover, they aim to provide a rich set of Application Programming Interfaces (APIs) that enable users and applications to interface with blockchains. To this aim, the Hyperledger architecture comprises of the following components, and as defined in [43] [27], categorized into various layers (see Figure 5):

- **Distributed Ledger layer** contains components to store the blockchain and the state of the data maintained by each of the peers. This bottom-most layer specifically consists of the following components.
  - **Communication** – responsible for peer-to-peer message exchange between the nodes that participate in a shared ledger instance. Several network protocols are supported.
  - **Consensus** – generates an agreement on the order and confirms the correctness of the set of transactions that constitute a block. To ensure that any Hyperledger framework can work with any consensus module, Hyperledger reaches consensus by performing two logically separate activities: ordering of transactions and validating transactions (as discussed below).
  - **Crypto abstraction** – allows swapping of different cryptographic algorithms or modules without influencing the functioning of other modules.
  - **Ledger storage** – ensures data storage and use of various data-stores across modules.
- **Smart contract layer** is responsible for processing transaction requests and determining if transactions are valid by executing business logic.
- **Membership layer** authenticates, authorizes and manages identities on a permissioned network. The identity management[11] component enables establishment of a root of trust during setup of a blockchain instance, enrolment and registration of identities, and management of changes like drops, add, and revocations. Other components within this layer provide authentication and authorization to various network participants and transactions.

[10] Following the notion in [42], 'Classic' is an established business and an 'Innovator' is a new organization whose primary focus is blockchain in some form or the other.

[11] The notion of identity is specifically significant in private and permissioned type blockchain. The **ISO/TC 307** on Blockchain and Distributed Ledger Technologies has created a working-group **WG 2 Security, privacy and identity** to promote standardization activities in this domain (see Chapter 5).

The membership and smart contract layers are together responsible for the management of various policies specified in the system, such as the endorsement policy, consensus policy, or group management policy.

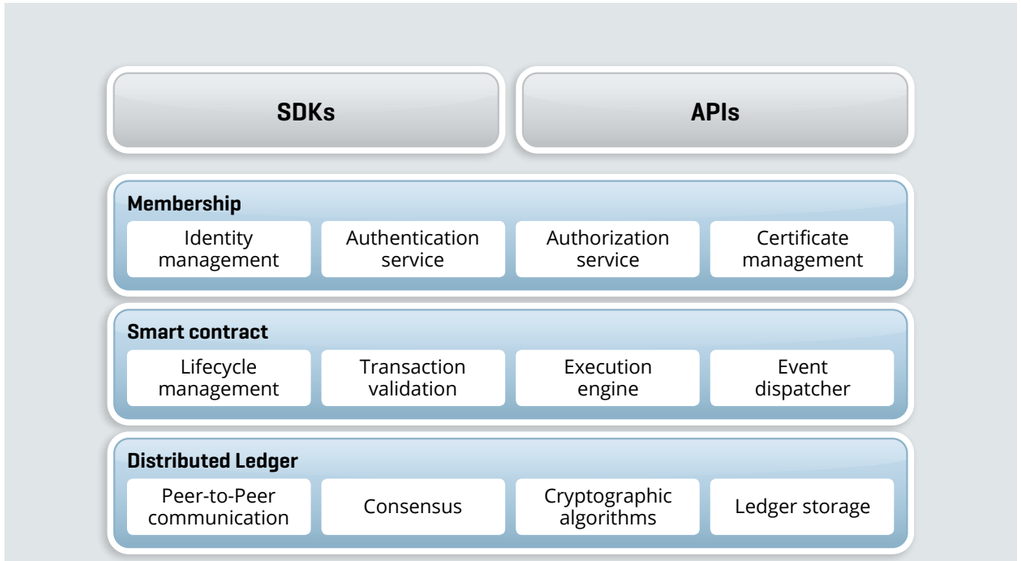


Figure 5: Hyperledger architecture [43]

Figure 6 illustrates a generalized view of the overall workflow/process within Hyperledger, based on [43]. However, given that Hyperledger frameworks are designed independently to serve specific set of goals, some steps within this process may vary with each framework.

As mentioned above, Hyperledger logically decouples two activities namely ordering of transactions and validating transactions to achieve consensus, and by doing so, ensures that any framework can work with any consensus module supported by Hyperledger. The ordering of transactions is performed at the distributed ledger layer (within the consensus component) and transactions validation is performed at the smart contract layer (see Figure 5) because it contains the business logic behind what makes a transaction valid.

The consensus component allows ordering of transactions to be implemented in different ways ranging from a centralized service to distributed protocols that target certain network and node fault models. It uses the communication component for communicating with the client and other peers on the network.

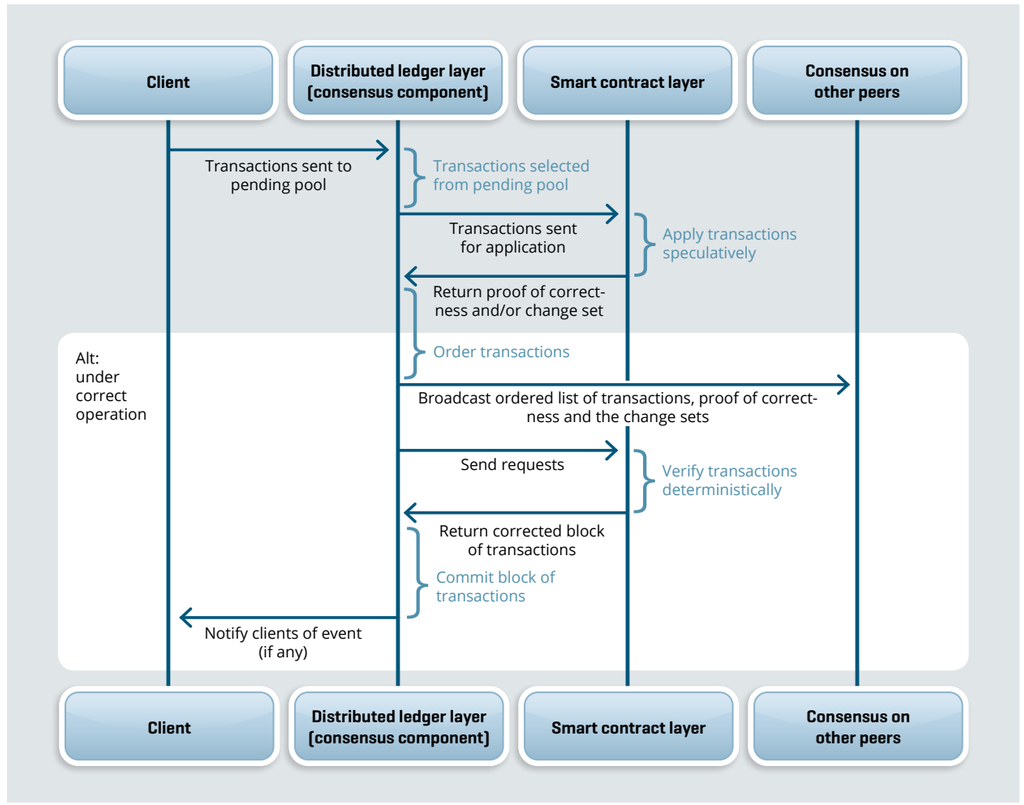


Figure 6: Typical workflow / process in Hyperledger [43]

The first step of the process consists in receiving transactions from the client application. Transactions are typically provided via a pre-defined interface to the consensus component, which collects transactions based on the consensus algorithm and configuration policy (e.g., that may define the number of transactions allowed and/or time limit). In general, to improve efficiency, transactions are grouped together in a block rather than working on individual transactions (see Figure 1). The smart contract layer then validates each transaction by verifying that it conforms to policy specified for the transaction. Invalid transactions are rejected and dropped from inclusion within a block. Potentially, two types of validation errors can occur: syntax and logic errors:

- The transaction is typically pruned for syntax errors (e.g., invalid inputs, unverifiable signature, and repeat transactions).
- Logic errors take a policy driven approach to decide whether to continue processing or not. For example, a transaction that would result in double-spend might be logged for auditing if the policy requires.

After successful validation process, the consensus component ensures deterministic ordering of transactions and broadcasts the list of transactions, proof of correctness as well as the change sets to the peers in the network. This triggers the final verification process and transactions/block is committed to the ledger.

2.3 Ethereum

Ethereum is one of the most successful open-source public blockchain projects, with contributions from many people around the world. It allows users to create their own operations (smart contracts) and serves as a platform that allows users to deploy and use different types of decentralized applications that run on blockchain [44]. These features have created an opportunity for businesses to realize projects that were infeasible earlier. For example, **Luxembourg Stock Exchange** has developed a decentralized application to ensure the authenticity and proof of existence of documents based on Ethereum platform [45]. Similarly, cryptocurrency wallets [46], smart locks [47], social media platforms with economic incentives [48] as well as electric car charging management system [49] are using Ethereum, to name a few.

2.3.1 Background

In a white paper published in 2013, Vitalik Buterin [19] proposed Ethereum as a means for building decentralized applications using general scripting languages. Formal development of Ethereum started in 2014 through a company called Ethereum Switzerland GmbH. Later, non-profit Ethereum Foundation was established, which was initially funded by an online public crowdsale – Initial Coin Offering (ICO) – where participants bought Ethereum cryptocurrency token (ether) with bitcoin (see Chapter 4 for details on ICO). This sale collected 31,591 bitcoins, worth $18,439,086 at that time, in exchange for 60,102,216 ether.

Developer interest in Ethereum grew steadily and the team delivered a series of prototypes for the community to evaluate. The last of these prototypes culminated in a public beta pre-release known as Olympic. Table 8 outlines Ethereum development roadmap. After Olympic, the Foundation announced the launch of Frontier as the next experimental release of Ethereum platform. Since the initial launch, several protocol upgrades/milestones were undertaken, resulting in Ethereum evolution with several important changes affecting the underlying functionality and/or incentives distribution policy of the platform. The **Homestead milestone** is considered **stable at the time of writing this chapter** and details given below are based on the documentation [39] of this milestone.

Version	Code name	Launch date
Pre-release Step 0	Olympic testnet	May 2015
Release Step 1	Frontier	30 July 2015
Release Step 2	Homestead	14 March 2016
Release Step 3	Metropolis (vByzantium)	October 2017
Release Step 3.5	Metropolis (vConstantinople)	TBA
Release Step 4	Serenity	TBA
Old version; not currently supported	Latest/current version (stable)	Planned future releases

Table 8: Ethereum development roadmap

In 2016, a startup called The DAO (Decentralized Autonomous Organization) that was building a humanless venture capital firm that would allow investors to make decisions through smart contracts was funded through a token sale and raised around $150 million from thousands of people [50]. Later, The DAO was hacked by an unknown attacker who stole ether worth $50 million dollars at that time. This event triggered a debate about whether or not Ethereum should perform a contentious hard fork to reappropriate the stolen funds. Note that creation of hard fork goes against the fundamental principles of blockchain and its properties of being immutable, tamper-proof, secure and anonymous. Eventually, the network split into Ethereum and Ethereum Classic [51]. Both blockchains have the same features and are identical to a certain block where the hard fork was implemented. After the hard fork related to The DAO, Ethereum was forked twice at the end of 2016 to defend against other attacks and to improve its protection against DDoS and spam attacks.

In March 2017, around 30 Fortune 500 enterprises, start-ups, research groups and ICT providers formed the **Enterprise Ethereum Alliance (EEA)**[12] to define enterprise-grade blockchain software. The goals of EEA are threefold: i) to define a roadmap for enterprise features and requirements; ii) to provide resources for businesses to learn about Ethereum and use it to address industry specific use cases; and iii) to define governance models and accountability, IP and licensing models for this open source technology. By July 2017, almost 150 members joined this non-profit alliance, making it one of the largest.

After this brief overview on the background of Ethereum, the rest of this section provides some technical details on its core components, based on [44].

2.3.2 Technical details on core Ethereum components

As mentioned above, Ethereum is designed to let users create their own operations (smart contracts) and to run decentralized applications on blockchain. In this context, a smart contract is a collection of code (functions) and data (its state) that resides at a specific address on the blockchain. It is typically written in a high-level language such as Solidity (or Serpent, LLL)[13], and compiled into an Ethereum-specific binary format called the EVM bytecode. This bytecode executes on the blockchain within an Ethereum Virtual Machine (EVM).

The notion of **accounts** is closely associated with smart contracts execution. As illustrated in Table 5, Ethereum adopts an **account-based data model**. This implies that an account is a basic unit and, if we view Ethereum as a state transition system, the states comprise **accounts** and state transitions represent transfer of value and information between accounts. There are two types of accounts: **Externally Owned Accounts** (EOAs) and **Contract Accounts**. The functionalities and differences between these account types are outlined in Table 9.

[12] https://entethalliance.org/

[13] Solidity is a language similar to JavaScript. It is currently the flagship language of Ethereum. Serpent and Lisp Like Language (LLL), on the other hand, are similar to Python and Assembly.

Externally Owned Accounts (EOAs)	Contract Accounts

• Has ether balance
• Has no associated code
• Can send transactions (e.g., ether transfer, trigger contract code)
• Controlled by private keys (and as a consequence, directly by human users who hold the private keys)
	• Has ether balance
	• **Has associated code**
	• **Code execution** is triggered by transactions or messages received from other contracts
	• Controlled by the internal **contract code**. A user controls a Contract Account only if it is programmed to be controlled by an EOA, with a certain address
	• When executed:
	  ▪ perform operations of arbitrary complexity (Turing completeness),
	  ▪ manipulate its own persistent storage i.e., can have a permanent state, and
	  ▪ can call other contracts

Table 9: Account types in Ethereum; their properties and differences [44]

Contract accounts, in other words, are able to pass messages between themselves and perform Turing complete computation. All other components of Ethereum are discussed below.

Ethereum network and clients: As expected, Ethereum includes a peer-to-peer network protocol that enables many nodes in the network to maintain and update the blockchain database. To become a node in the network, the first step consists in running an Ethereum client. An Ethereum client provides a number of methods over JSON-RPC that an application can use and this task is simplified by means of web3.js[14], web3j[15], Nethereum[16] and Ethereum-ruby[17] libraries.

Mining: Since Ethereum is public and permissionless, any node in the network is allowed to be a miner. In concurrence with typical blockchain concepts, miners group **transactions** into blocks and collect **transaction fees**. Ethereum currently uses Proof-of-Work in the **mining process** but has announced that a hybrid system called Casper that merges Proof-of-Work (PoW) with Proof-of-Stake (PoS) is under development, and the new system will replace the current one in Metropolis milestone [39]. Chapter 1 describes the notions of PoW and PoS.

The PoW algorithm in Ethereum is called Ethash, which is a modification of Dagger-Hashimoto algorithm, and consists in finding a nonce such that the result remains below a certain difficulty threshold. The difficulty is dynamically adjusted in order to maintain the average rate of production by the entire network to one block in every 15 seconds [44] [2]. Ethash ensures synchronization of system state and guarantees that maintaining a fork or rewriting history by malicious actors are impossible unless the attacker controls more than half of the network mining power. Differently from bitcoin that experiences certain degree of centralization due to the use of specialized hardware (e.g. ASICs) by miners, Ethereum provides memory-hard computational problems. The basis of this idea is that general computers are best suited to solve problems that require both memory as well as CPU. This makes Ethash ASIC-resistant.

[14] https://github.com/ethereum/web3.js/

[15] https://github.com/web3j/web3j

[16] https://github.com/Nethereum/Nethereum

[17] https://github.com/DigixGlobal/ethereum-ruby

The fees collected by miners can be viewed as a compensation for dedicating hardware and electricity to the Ethereum network and for winning the competition (PoW) among miners for including their block as the next one in the blockchain. The expected revenue from mining will be directly proportional to their relative mining power (the number of nonce tried per second normalized by the total hashrate of the network). Overall, the successful PoW miner of the winning block receives:

- A static block reward of 5 **ether** for the winning block.
- The cost of the **gas** spent within the block (an equivalent amount of ether based on the current gas price is given).
- Additional reward of 1/32 per uncle for including uncles as part of the block. Uncles are stale blocks with parents that are ancestors of a maximum of six blocks of the including block.

Gas and ether: Gas represents the execution fee that senders of transactions pay for operations made on Ethereum blockchain. The following are terms often associated with it [44]:

- **Gas Cost** is a static value denoting how much a computation costs in terms of gas. The goal is to maintain the real value of gas stable over time.
- **Gas Price** indicates the value of gas in terms of another currency or token like ether. The Gas Price is a floating value such that if the cost of ether (or currency) changes, the Gas Price adapts to keep the same real value. The goal is to maintain an equilibrium price that users are willing to spend and processing nodes are willing to accept.
- **Gas Limit** represents the maximum amount of gas that a block can use. It includes the maximum amount of computational load, transaction volume, and block size of a block. Miners can steadily change this value over time.
- **Gas Fee** is the amount of gas to be paid to the miners for running a particular transaction or program (called a contract).

For example, consider a smart contract that adds 2 numbers and assume that the corresponding EVM opcode consumes 3 gas. If the gas price is 0.05e12, then the approximate cost would be: 3 * 0.05e12 = 1.5e11 wei. Given that 1 ether is 1e18 wei, the total cost would be 0.00000015 Ether (see Table 10).

Ether is the name of the currency (token) used in Ethereum [44]. It is used to pay for computation within the EVM, which is done indirectly by purchasing gas for ether. Ethereum has a metric system of denominations used as units of ether. The smallest denomination called the base unit of ether is called Wei. Table 10 gives the list of named denominations and their value in Wei. Following a similar pattern, ether also designates a unit (of 1e18 or one quintillion Wei) of the currency.

Unit	Wei value	Wei
Wei	1 wei	1
Kwei (babbage)	1e3 wei	1,000
Mwei (lovelace)	1e6 wei	1,000,000
Gwei (shannon)	1e9 wei	1,000,000,000
Microether (szabo)	1e12 wei	1,000,000,000,000
Milliether (finney)	1e15 wei	1,000,000,000,000,000
Ether (= €260 on 1st Nov 2017)	1e18 wei	1,000,000,000,000,000,000

Table 10: Denomination in Ethereum [44]

Three possible ways of obtaining ether are:

- By becoming Ethereum miner (and participating in the mining process),
- By trading other currencies for ether using centralized or trustless services, and
- By using Mist Ethereum GUI Wallet that as of Beta 6 introduced the ability to purchase ether using the http://shapeshift.io API. Several exchanges that serve as platforms to buy and sell cryptocurrencies for fiat currencies or other cryptocurrencies now trade in ether (see Section 4.1).

Transactions and messages: A transaction refers to the signed data package that stores a message sent by an EOA. A transaction contains the following information [44]:

- The identity/address of the recipient of the message,
- A signature identifying the sender,
- The amount of ether to transfer from the sender to the recipient,
- An optional data field,
- A STARTGAS value, representing the maximum number of computational steps the transaction execution is allowed to take, and
- A GASPRICE value, representing the fee the sender pays per computational step.

The first three fields are standard and as expected. The data field is optional and has no function by default. However, it has an opcode that an EVM can use to allow a **contract** to access data (see Contract Accounts above).

As discussed above, the fundamental unit of computation in Ethereum is called **gas**. Each transaction sets a limit on the number of computational steps that the transaction can use, based on the STARTGAS field. A typical computational step for instance could cost 1 gas and an expensive computational step could cost higher amounts of gas. Users must pay a small transaction fees to the network (e.g., 5 gas for every byte in transaction data), as indicated by the GASPRICE field. This protects the Ethereum blockchain from frivolous or malicious computational tasks and ensures that attackers pay proportionately for every resource that they consume, including computation, bandwidth and storage [44]. Chapter 3 analyzes vulnerabilities that result in malicious use of gas.

2.4 Stellar

While Ethereum has extensive capabilities, some applications require only a subset of its features, and Turing completeness as well as support for complex smart contracts become extraneous. For instance, many Initial Coin Offerings require only basic tokens and not all capabilities of Ethereum. At the same time, several platforms for specific domains (e.g., payments) are being developed and customized for high performance and usability in that domain. Stellar is an example of such a platform [52]. It connects banks, payment systems and people, and ensures quick, reliable and cost-effective transfer of money. This section investigates Stellar in detail and serves as a reference for an industry-specific platform in this white paper (in contrast to general-purpose platforms – Hyperledger and Ethereum – discussed earlier).

2.4.1 Basic concepts, Stellar network, and Stellar.org

As shown in Table 5, accounts are the central database structure in Stellar, similarly to Ethereum. The Stellar ledger records a list of all the balances and transactions (e.g., offers made for buying and selling currencies) belonging to every single account on the network. These offers represent commitments to exchange credit (including, one type of credit to another at a pre-determined rate) and given that the ledger is public, Stellar enables a global marketplace for offers. Internally, Stellar maintains an order book comprising offers for each currency/issuer pair. For example, a specific order book in the ledger allows users to see an exchange from BankName/Euro to CompanyName/Bitcoin. This allows users to not only buy and sell currencies similarly to a traditional foreign exchange but also to convert currencies seamlessly during transactions.

A copy of the ledger is hosted on each server that runs **Stellar Core**. Stellar Core implements the Stellar Consensus Protocol (see Section 1.5), maintains a local copy of the ledger, and remains in sync with other instances of the Stellar Core in the network. Different individuals and entities around the world maintain these servers, forming a decentralized network, referred to as the **Stellar Network**.

The Stellar network allows users to build a range of **applications** involving payments (e.g., mobile wallets, banking tools, smart devices that pay for themselves). As shown in the Figure 7, applications interact with the Stellar network through a server called **Horizon**. This server allows users to submit transactions, check accounts and subscribe to events. Users can communicate with Horizon using web browser, command line tools like cURL, or the Stellar SDK. Stellar.org provides a SDK supporting JavaScript, Java as well as Go programming languages; while the community maintains SDK supporting Ruby, Python and C#. Internally, Horizon connects to **Stellar Core**, which in turn validates and agrees with other instances of Core on the status of every transaction. Each transaction on the network costs a fee of 100 stroops (0.00001 XLM – Stellar's native currency Lumen)[18] that is aimed at reducing network spamming. A docker image can be used to install Horizon and Stellar Core[19].

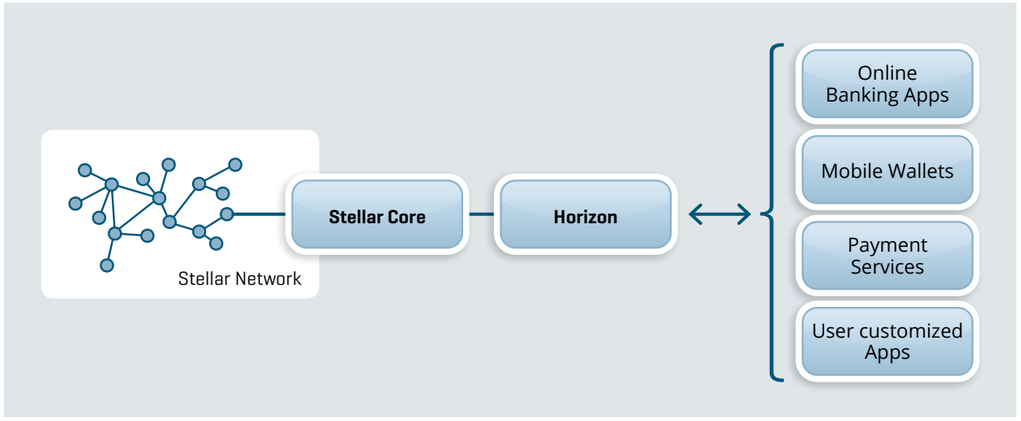


Figure 7: Stellar overview

While the **Stellar Network** refers to the open source, distributed, and community owned technology, **Stellar.org** is the nonprofit organization that contributes to the development of tools and social initiatives around the Stellar network and financial inclusion[20]. Although employees contribute code to the Stellar network, the technology is independent of the organization.

[18] https://www.stellar.org/developers/guides/concepts/fees.html

[19] https://hub.docker.com/r/stellar/quickstart/

[20] http://www.ibtimes.co.uk/leaping-into-future-nigerias-rural-microfinance-community-gets-connected-using-stellar-oradian-1541238 as an example

2.4.2 Anchors in Stellar network

Anchors are entities in the Stellar network that are trusted to[21]:

- Take a user's deposit and issue corresponding credit to the user's **account** on the Stellar ledger;
- Allow users to make withdrawals by obtaining credit issued to them.

In other words, all money transactions in the Stellar network (except the native digital currency of lumens) occur in the form of credit issued by anchors.

Consider a traditional payments service such as Paypal as an example. Users deposit money from their bank accounts to Paypal accounts and gain Paypal credit. This credit can then be sent to anyone who has a Paypal account. The receiver of the credit can convert it to currency/real money by withdrawing it from the bank.

Anchors have the same role in the Stellar network. However, a notable difference is, all payment services and corresponding anchors operate on the same network, making it easy to send and exchange different anchor credits with each other. Table 11 lists Stellar anchors[22].

Name of the organization	Country	Currency	Focus area
Bloom	Philippines	PHP	Remittance
Cellulant	Nigeria	NGN	Payment and digital commerce
Coins	Philippines	PHP	Mobile financial service provider
DBT	Uganda, Rwanda	UGX	Digital payment and banking
Fair-eZone	Europe	EUR	Money transfer
FCMB	Nigeria	NGN	Whole banking
Flutterwave	Nigeria, Kenya	NGN, KSH	Digital payment infrastructure
ICICI Bank	India	INR	Integrating banking and Stellar network to support money transfers
KlickEx	Pacific Region	Multiple	Cross-border payments
NaoBTC	World	BTC	BTC transfer and other digital assets exchange
Parkway Projects	Nigeria	NGN	Financial technology provider
RippleFox	China	CNY	CNY anchor that allows sending money to any bank or Alipay account in China
SendX	Singapore	SGD	Money transfer globally
Splash Mobile Money	Sierra Leone	SLL	Mobile payment system
TEMPO	France	EUR	European licensed remittance provider operating in 43 countries

Table 11: Anchors in Stellar network

[21] https://www.stellar.org/how-it-works/stellar-basics/explainers/#Anchors_trust_and_credit

[22] https://www.stellar.org/about/directory

An anchor's infrastructure must support the following activities:

- Make payments.
- Monitor a Stellar account and update user accounts when payments are received.
- Look up and respond to requests for federated addresses.
- Comply with Anti-Money Laundering (AML) regulations.

Stellar provides a **federation server** and a **regulatory compliance server** that an anchor can use within its infrastructure. It can also write its own customized versions, if necessary. Stellar.org also maintains a **bridge server** to simplify usage of federated and compliance servers for sending and receiving payments:

- The **federation server** is the Go implementation of the federation protocol. While federation allows a single Stellar account to represent multiple people/users, the Stellar federation protocol allows conversion of a human-readable address (e.g., abc*some_org.com) to a Stellar account ID.
- Complying with Anti-Money Laundering (AML) laws requires financial institutions to know not only who their customers are sending money to but also who their customers are receiving money from. Certain jurisdictions allow banks to trust AML procedures of other licensed banks while others require each bank to do its own sanction checking of both the sender and the receiver. The Compliance Protocol handles all these scenarios. The **compliance server** is a stand-alone server, also written in Go, that is designed to make compliance protocol requests to other organizations.

2.4.3 Sending and receiving payments[23]

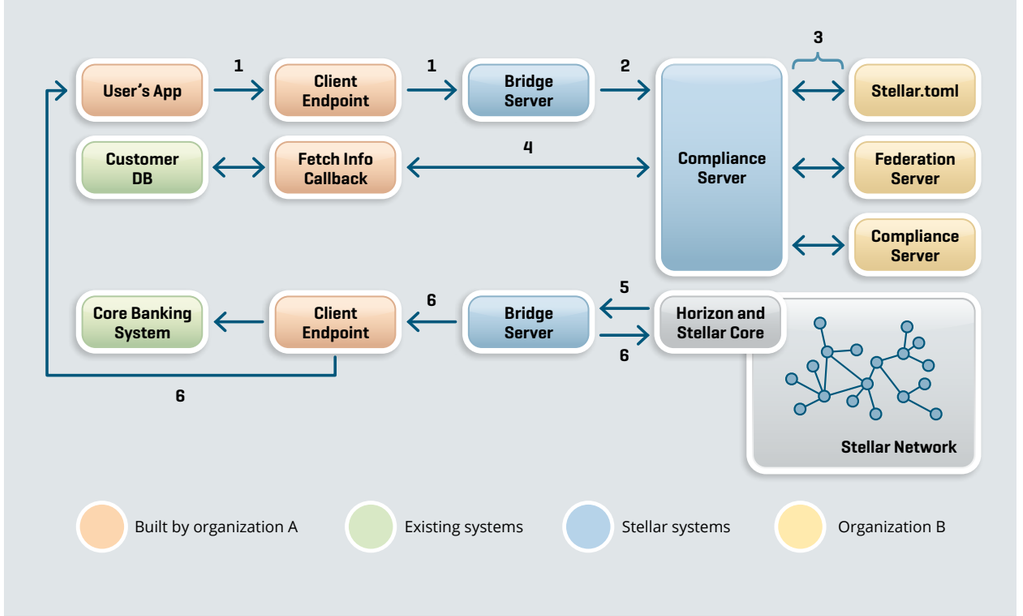


Figure 8: Sending payment using Stellar

[23] https://www.stellar.org/developers/guides/get-started/transactions.html

Sending payments (from A to B): A complex payment can be made using Stellar, and its bridge, federation and compliance services, as follows:

1. A customer (from organization A such as a bank) fills out a payment request using A's mobile app or a website. The Client UI (user interface) of the app sends the request to the Client Endpoint, which in-turn forwards it to the bridge server.
2. The bridge server determines the need for compliance checks; if true, it forwards transaction information to the compliance server.
3. The compliance server determines the receiving account ID by looking up the federation address.[24]
4. Then, it gets information about the customer sending the payment in order to provide it to the receiving organization's compliance systems.
5. If the result is successful, the bridge server finally creates a transaction, signs it, and sends it to the Stellar network.
6. Once the Stellar network confirms the transaction, the bridge server returns the result to the Client Endpoint, which updates customer's account.

Receiving payments: While receiving a payment from a customer of organization B to A, the flow of activities is as follows:

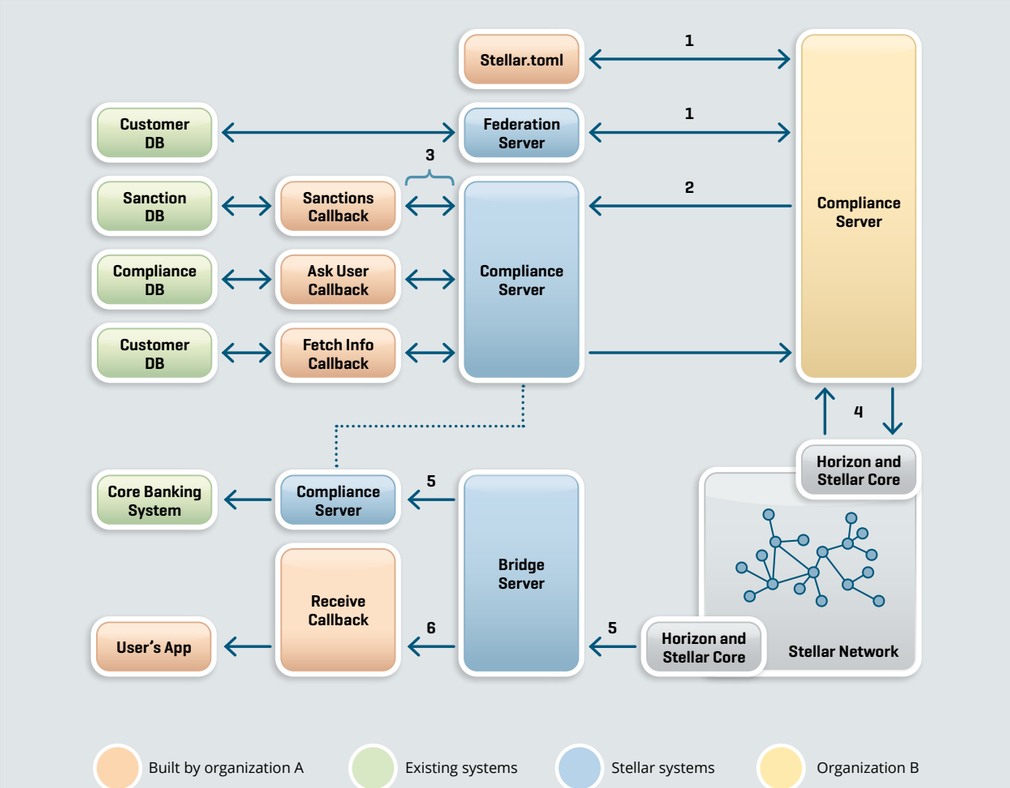


Figure 9: Receiving payment using Stellar

[24] The stellar.toml file is used to provide a common place where the Internet can find information about a given domain's Stellar integration. Any website can publish Stellar network information.

1. B fetches the account ID to send the payment to (using stellar.toml), and obtains A's federation and compliance URLs.
2. B contacts the compliance server of A with information about the customer sending the payment.
3. Then, B's compliance server contacts three services:
   a. A sanctions callback to determine whether B's customer is permitted to pay to the customer of A.
   b. If B wants to check A's customer information, a callback is used to determine whether A is willing to share this information.
   c. The same callback is useful when sending a payment.
4. The sender B submits the transaction to the Stellar network.
5. The bridge server monitors the Stellar network for the transaction and sends it to A's compliance server in order to verify if it was the same transaction that was approved in Step 3a.
6. The bridge server notifies A about the transaction. Organization A can use this information to update its customer's account balances.

2.4.4 Use cases

Several financial institutions, payment aggregators and technology experts have integrated to, are working with, or are supporting the Stellar network with the aim of building a global infrastructure for payments. These companies include Stripe, Wanxiang Blockchain Labs, bext360, Gingkoo, Whiterock, Wipro, Hijro, Telindus and many others[25]. For instance, Stellar is being used to: i) decrease the cost of smaller transfers and to offer incremental payment options (by Deloitte)[26], ii) lower the cost of remittance (by Tempo)[27], and iii) make mobile money platforms interoperable (by Parkway)[28].

In October 2017, IBM revealed the results of its partnership with Stellar in which it successfully settled real transactions using the lumens cryptocurrency. The payments were conducted for the Advancement of Pacific Financial Infrastructure for Inclusion (APFII), an organization of member financial institutions founded by the United Nations and Swift, and operated by KlickEx, a privately-held direct clearing provider that specializes in cross-border digital remittances[29].

Initial Coin Offerings are gaining an increasing popularity as a fundraising model for new businesses, particularly in the blockchain industry. Section 4.1.1 provides detailed insights on ICOs. Traditionally, ICO tokens have been issued using Ethereum network but this model has recently highlighted some shortcomings such as slow transaction processing times and expensive gas prices. Consequently, Stellar is being pitched as the best alternative for ICOs [52].

[25] https://www.stellar.org/about/directory#companies

[26] https://www2.deloitte.com/mt/en/pages/about-deloitte/articles/mt-pr2016-008-deloitte-blockchain-initiative-with-five-tech-companies-and-20-prototypes-in-development.html

[27] https://www.wired.com/2016/12/bitcoin-stellar/

[28] https://www.stellar.org/how-it-works/powered-by-stellar/#Parkway

[29] https://www.coindesk.com/ibms-stellar-move-tech-giant-use-lumen-cryptocurrency-payments-rail/

2.5 Insights on blockchain related initiatives

An interesting trend in the areas of blockchain and distributed ledger technologies indicates that a growing number of companies, regulators, and governments are realizing their blockchain strategy as part of consortia. In a way, this is a just trend given that distributed ledgers streamline business-to-business workflow, demanding mutual agreement on standards, infrastructure, and transactions execution. Since these consortia are one of the primary sources of blockchain development, this section provides a set of insights that might help readers in gaining deeper understanding of the area.

Insight 1: By October 2017, around 40 consortia have been formed globally, and they can be classified as being technology-focused or business-focused [53]. The former class of consortia aims at developing reusable blockchain platforms based on technical standards. The two most successful technology-focused blockchain consortia, as discussed in Sections 2.2 and 2.3, are Enterprise Ethereum Alliance (EEA) and Hyperledger respectively. Business-focused consortia, on the other hand, aim at building and operating blockchain platforms to solve specific business problems. An example is FundChain, launched in summer 2016 by ten key market players of the fund industry, and aims at "developing solutions using distributed ledger technology and smart contracts to act as innovation pioneers for the fund distribution value chain in Luxembourg". A third class of consortia cover both types of activities. For example, more than 80 financial institutions, regulators, and central banks are developing the Corda platform as part of the R3 consortium.

Insight 2: The first set of consortia (R3 Distributed Ledger Consortium and Digital Asset Holdings), formed in 2014, focused on financial services. Similarly, Hyperledger was one of the first technology-focused consortia formed in December 2015. Year 2016 witnessed formation of many different consortia, some to develop blockchain and DLT within a country (e.g., UAE's Global Blockchain Council; see Insight 4), most focusing on financial services[30] and others in specific economic sectors like logistics, healthcare, insurance etc. (Insight 3). The interest in blockchain continued to grow through year 2017. However, these consortia focus more on cross-sectoral use of blockchain rather than financial services alone.

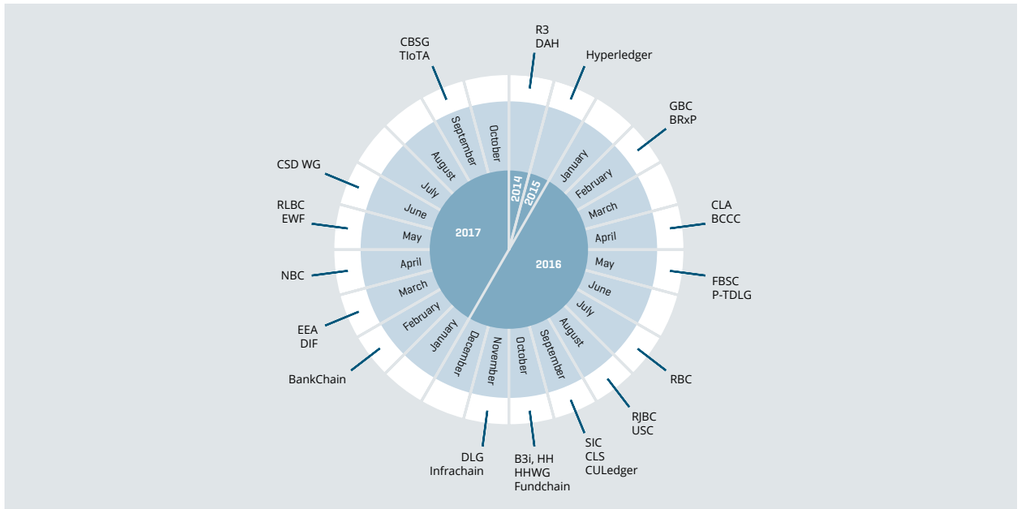


Figure 10: Timeline of formation of blockchain consortia

[30] Examples: RJBC – Ripple Japanese Bank Consortium, USC – Utility Settlement Coin, RBC – Russian Banks Consortium, FBSC – Financial Blockchain Shenzhen Consortium, P-TDLG – Post-Trade Distributed Ledger Group, Fundchain, SIC – Swiss Industry Consortium, CLS Blockchain Consortium, CULedger Credit Union Consortium.

Insight 3: As discussed in Insight 2, while a majority of consortia focuses on financial services, other sectors such as telecommunications, logistics, energy and healthcare are also following the trend. Some notable consortia of this kind (at the time of writing this chapter) are:

Name of the consortium	Sector	Number of members	Notes
Energy Web Foundation (EWF)	Energy	12	Co-founded by Rocky Mountain Institute and Grid Singularity. Companies that are part of the consortium include Centrica plc, Elia System Operator, ENGIE Group, Sempra Energy, Shell, SPgroup, Statoil, Stedin B.V., TEPCO, TWL Meine Energiequelle. EWF is a non-profit focussed on accelerating blockchain technology across energy sector. Launched a test network in October 2017.
HashedHealth (HH)	Healthcare	NA	Commercialization of blockchain on healthcare; activities range from regulatory compliance, development, medical records management, insurance, payments and claims lifecycle.
Hyperledger Healthcare Working Group (HHWG)	Healthcare	5	Build blockchain applications for healthcare space. Members involved in this working group are Accenture, Gem, Hashed Health, Kaisser Permanente, IBM.
Carrier Blockchain Study Group (CBSG)	Telecommunications	4	This group has so far tested systems for mobile payment and recharging prepaid phones. Members include Sprint, Softbank, FarEasTone and TBCASoft. This group also plans to release IoT applications.
Decentralized Identity Foundation (DIF)	Personal Identity	30	The goal of this group is to build an ecosystem around decentralized identities that are anchored by blockchain IDs, linked to zero-trust datastores and that are universally discoverable. www: http://identity.foundation/
Dutch Logistics Group (DLG)	Logistics	16	Study efficacy and efficiency of blockchain in reducing supply chain footprints. Members: TKI Dinalog, TU Delft, ABN Amro, SCF Community, Port of Rotterdam, Royal Flora Holland, SmartPort, Windesheim, TNO, Centric, Exact, FBBasic & Cirmar, BeScope Solutions, NBK, Innopay and TransFollow.
Trusted IoT Alliance (TIoTA)	IoT	18	Formally announced in September 2017. This foundation aims to support the creation of a secure, scalable, interoperable, and trusted IoT ecosystem. By 2025, the goal is to, on the one hand, accelerate the digitalization of products, assets, and machines for frictionless M2M and supply chain interactions. On the other hand, support the automotive, pharma, drone, smart card, postal system, supply chain, industrial IoT, insurance, and emerging machine, and autonomous economies. www: https://www.trusted-iot.org/
B3i	Insurance	15	This is one of the largest and most successful consortium focusing on insurance and reinsurance challenges. In September 2017, a beta prototype was released through which productivity gain of up to 30% was observed. In 2018, the group plans to move towards real contracts, real data and parallel run. www: http://b3i.tech/home.html
CSD Working Group (CSD WG)	Central Securities Depositories	6	This association is working on developing reference products using DLT. It has released product requirements for proxy voting business case in April 2017, in alignment with ISO 20022. Members include Moscow Exchange Group, SIX Securities Services, Nordic subsidiary of Nasdaq, DCV, Strate and Caja De Valores.

Table 12: Notable blockchain consortia in non-finance sectors

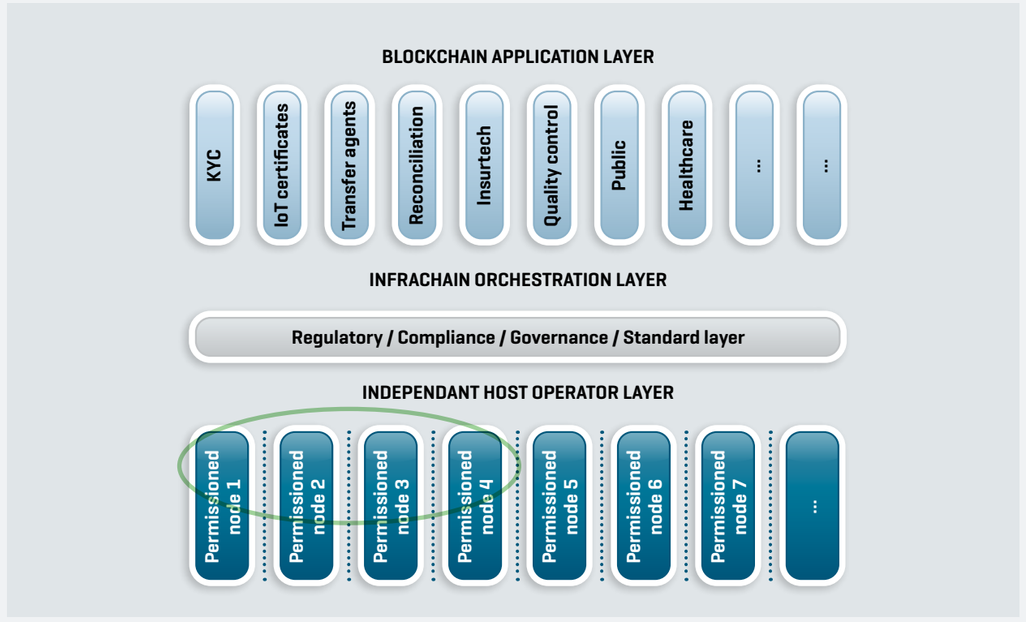
Insight 4: Several national (Luxembourg, Japan, UAE, Spain, China, The Netherlands) consortia are formed to advance the development and adoption of blockchain across multiple sectors:

- **Infrachain** was formed in November 2016 in **Luxembourg** with a threefold mission:
  - Leapfrog the adoption curve of blockchain by creating a compliant-ready community and permissioned node blockchain infrastructure.
  - Provide disintermediation services to all aspects of the economy (e.g., fintech, healthcare, public services, supply chain management).
  - Create a vibrant European community of blockchain professionals driving and shaping the future blockchain industry.

  Founding members of this initiative are Abacus Consulting & Solutions, Affidaty S.p.A., Allen & Overy, Ant Financial, Banque et Caisse d'Epargne de l'Etat (BCEE), Bitbank, Cambridge Blockchain, CoinPlus, Computer Task Force (CTG), CTIE, Deloitte Luxembourg, eGaaS, Finimmo Luxembourg S.A., Grant Thornton, InTech S.A., KPMG, KYC3, LuxTrust S.A., Netis blockchain technologies, Page Solutions, Pingvalue, Scorechain, Snapswap, SunContract and Telindus.
- 34 companies formed the **Blockchain Collaborative Consortium (BCCC)** in **Japan** in April 2016. Today, BCCC comprises 146 companies and is involved in a range of activities including educating the public, researching and developing, and promoting investment in the blockchain technology as well as working together with blockchain organizations overseas.
- In February 2016, the **Global Blockchain Council (GBC)** was formed under Public-Private Partnerships among businesses, the **government of UAE** and startups. Several prototypes in a range of sectors have been unveiled: health records, diamond trade, title transfer, business registration, digital wills, tourism engagement and improved shipping.
- A group of 22 **Spanish** organizations announced launch of **RedLyra Blockchain Consortium (RLBC)** in May 2017.
- **China** Ledger Alliance **(CLA)**, formed in April 2016, aims to develop blockchain technology and focuses on regulatory compliance and Internet of Everything. It has 11 members including Shanghai Stock Exchange.
- **Ministry of Economic Affairs, The Netherland**s, formed the National Blockchain Coalition (NBC) in April 2017. It currently has around 20 members.

Infrachain a.s.b.l.

Infrachain is a private sector initiative with support from the Government of Luxembourg. It has its origins in a Luxembourgish non-profit organization; but now, it strives to become a European non-profit organization putting in place community-driven governance for operational blockchain use. A strong and transparent governance is set within the community in order to distribute the power among members. The role of governance rules is to guarantee the independence of actors involved in the operation of blockchain instances. This is one of the main differentiators when compared to a cloud alternative offered on the market. Key features of Infrachain are summarized here:



- **Host operator (node) Certification** – to know all parties related to a blockchain application, Infrachain is providing an ISO/IEC 27001 inspired certification.
- To establish signed SLA towards blockchain applications, a "Last man standing" approach is used.
- The position of Infrachain and all its stakeholders is defined light of the GDPR.
- **Orchestration of private chain instances:** Automatic initiation of setup of blockchain instances on host operators' resources is possible through an orchestration layer.
- 3rd party distributed trust through a community of independent host operators is provided.
- Infrachain is **blockchain technology** agnostic and is ready to adapt its governance accordingly.

Infrachain already has 36 members from six EU member states. A stable test environment in Ethereum is available and it is a member of EEA and, since December 2017, a member of the Hyperledger project.

Insight 5: The pie chart in Figure 11 illustrates where (geographically) these consortia come from (e.g., BCCC among others come from Japan). In case a consortium involves several international members, the company leading the consortium (where information is available) and its headquarters is considered as location in this figure. For instance, R3 Distributed Ledger Consortium involves more than 100 organizations and is headed by R3 CEV, USA. Finally, note that this figure includes consortia focusing both on financial and non-financial sectors.

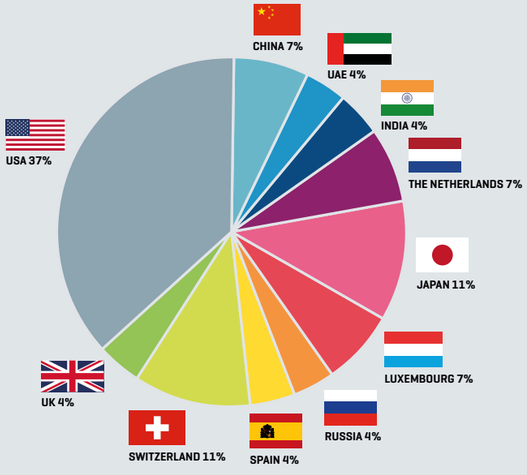


Figure 11: Geographical distribution of blockchain consortia

Insight 6: Figure 12 illustrates which countries are leading consortia in different sectors.

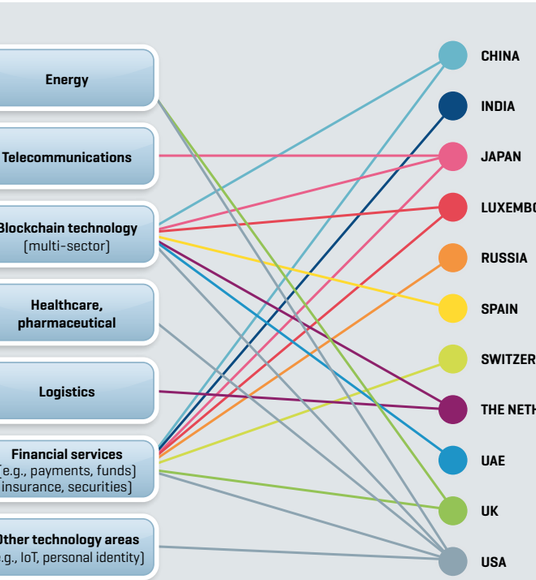


Figure 12: The sector(s) in which a country is leading blockchain consortium

Insight 7: Major companies such as Microsoft and IBM are also transforming the outcomes (e.g., blockchain platforms such as Ethereum and Hyperledger Fabric) of these consortia to enterprise-grade products and services. For instance, both Microsoft (through Coco Framework [54]) and IBM[31] are offering a suite of cloud services to help clients create and manage blockchain networks. These services are discussed in Section 2.6.1

2.6 Blockchain and Smart ICT

This section establishes the relationship between blockchain and Smart ICT namely Cloud computing, Internet of Things and Big data to understand blockchain from an overall ICT ecosystem point of view. Section 5.6 summarizes standardization activities relevant to blockchain and Smart ICT.

2.6.1 Cloud computing

Blockchain applications are highly resource intensive. For instance, the amount of electricity utilized by bitcoin mining is comparable to average power consumption of Ireland [30]. Similarly, the amount of networking resources (e.g., bandwidth) used to ensure consensus is significantly higher than typical centralized applications. This demand for computing resources, coupled with the necessity for scalability and flexibility in obtaining and managing those resources, has resulted in wide adoption of cloud computing services by blockchain solutions. Consequently, many cloud providers are offering cloud environments optimized for blockchain and are building the new paradigm of **blockchain as a service**.

For instance, IBM is offering cloud infrastructure services optimized for **cloud-based blockchain networks** by allowing auditable operating environment with comprehensive log data that is useful for forensics and compliance. Cryptographic keys are stored in a secure and tamper-resistant storage. Other supporting modules detect and respond to unauthorized attempts to access the keys. In addition, the IBM Bluemix **platform** is providing tools for rapid development and testing of blockchain applications.

Microsoft Azure is providing tools for building enterprise-grade blockchain solutions with improved security, performance and operational processes. Its data and AI platform is one of the few services that provides off-chain data management and analysis capabilities[32]. In August 2017, Microsoft also announced its Coco Framework that, when integrated with a blockchain network, provides [54]:

- Transaction speed of 1,600 transactions/second;
- Easily managed data confidentiality; and
- Distributed governance model for blockchain networks that establishes a network constitution and allows members to vote on all terms and conditions governing the consortium and the blockchain software system.

In contrast to cloud services that help blockchain networks and applications (above), many solutions have used blockchain to either improve trust in their cloud services or to build new innovative models. Storj Labs, for example, uses blockchains to create a peer-to-peer, decentralized, cloud storage system. It uses spare disk space offered by network nodes, who in turn receive rent in Storj's native cryptocurrency. Stored files are "shredded" and the shards encrypted and distributed across available storage using blockchain features.

[31] https://www.ibm.com/blockchain/offerings.html

[32] https://azure.microsoft.com/en-us/solutions/blockchain/

While Liang et al. [55] propose a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, Rimba et al. [56] compares blockchain and cloud services for business process execution. Other solutions such as [57] explore usage of blockchain features to ensure data integrity in cloud computing. **ISO/IEC JTC 1/SC 38** Cloud Computing and Distributed Platforms and **ISO/TC 307** Blockchain and Distributed Ledger Technologies are working in liaison to standardize these aspects (see Chapter 5).

The advent of cloud computing has also provided impetus to two paradigms (big data and IoT) that play vital roles in today's society as well as economy. In this context, the relationship between blockchain, big data and IoT becomes important and the rest of this section studies these aspects in detail.

2.6.2 Big data and analytics

The trend within blockchain development is similar to that of big data in the sense that the notion of big data came into existence when companies designed internet-scale computation frameworks such as BigTable, MapReduce, Cassandra etc. Then, open source projects like Hadoop started to build tools with support from developers from across the globe, some even backed by industry leaders. Finally, startups such as MongoDB transformed open source projects to enterprise-grade products and services. Currently, big data is transforming almost every enterprise, replacing data stores/warehouses with data lakes, relational databases to unstructured databases, Gigabytes of data to Petabytes, and so on, providing many new avenues for business opportunities.

By analogy, the notion of blockchain was derived from bitcoin; then, open source projects such as Ethereum and Hyperledger started building a range of tools/platforms. Several startups such as R3 and international companies like Microsoft and IBM then started to transform open source tools to enterprise-grade offerings. Now, blockchain is moving beyond financial services and exploring several other domains including logistics, Internet-of-Things, healthcare among others [58].

Current big data challenges: Typical big data applications face several challenges ranging from interoperability, scalability and data quality to trust, data monetization and authenticity. Some key big data challenges are discussed below [59]:

- **Trust:** Data needs to come from reliable sources to ensure high quality of analytical results. In the context of IoT, for instance, this requirements becomes challenging since sensors might crash or experience Byzantine failures. Similarly, there is a challenge on the one hand for data receivers in knowing whether the obtained data is truly authentic and on the other hand for data generators to prove the origin of the data to others.
- **Control over infrastructure:** The question of how to share control of the system (e.g., data stores) becomes critical for applications that involves participation of several stakeholders, who may sometimes be competitors.
- **Administration:** Data is often replicated/spread across different geographical locations to improve resilience/to support business needs. In this context, consistency of data and compliance to regulations become a challenge.
- **Monetization:** Ways to build new business models, rights over data, and the notion of universal data marketplace remain an open challenge.

Blockchain for big data and analytics: As discussed in Chapter 1, blockchain is a database that offers benefits such as decentralization, shared control and immutability. However, in comparison with databases currently used for big data applications (e.g., MongoDB), blockchains not only lack scalability and capacity but also fine-grained query languages and access control features (see Section 1.3). Recent (blockchain database) advancements such as BigchainDB are combining the benefits of traditional distributed databases and blockchains, and in this process, addressing several challenges that were earlier infeasible to be resolved. The opportunities created are discussed below in detail [58] [59]:

- **Decentralization/shared control:** Blockchain enables shared control of the database structure across the network. For example, let each office of a multinational enterprise control one node of the blockchain network; then, the enterprise implicitly maintains the database collectively and ensures consistency as well as availability of data even if one of the offices are under cyberattack.

  Moreover, decentralized/shared control results in better and qualitative models for data analytics, leading to higher profits. Consider a consortium of enterprises as an example. Since no single entity controls the infrastructure and the benefits apparent, each enterprise might be more willing to share data, as opposed to being in silos (the present situation). This combination of data from several enterprises would result in more data, and consequently, better models for analytics (e.g., identifying root causes of failure, fraud detection) and correlations (e.g., relation between quality of product and energy consumption pattern in a manufacturing unit) supported by artificial intelligence.
- **Immutability:** Data in a blockchain is stored in a chronological order in an append-only manner, making the database structure tamper-resistant and immutable. This property enables effective audit trials on data, as well as making provenance of information feasible.

  Consider a typical IoT workflow with steps such as data acquisition, event alerts, storage, pre-processing, normalization and analytics. At each step in the workflow, let a transaction is created (e.g., by including a hash, digital signature, time-stamp) and stored in the blockchain. The data owner can prove its origin or verify the authenticity of the data received by means of public key cryptography. Similarly, if a sensor is compromised and generates incorrect data, a periodic rehash of data can reveal inconsistency. This feature can be very useful, for instance, in catching leaks within a data supply chain.
- **Data and analytics models as an Intellectual Property (IP):** Consider a system that combines Coala IP[33] and a global public blockchain. Data (or data analytics model) rights could then comprise an asset that resides on the blockchain and the participant with the private key owns the asset. Note that the claim of IP would be a tamper-resistant global registry. Only the owner of the private key can transfer the asset to others, backed by standard IP laws, by means of a blockchain transaction.

Blockchain and big data use cases: A number of studies have explored the use of blockchain to address challenges within the big data paradigm. Most notable use cases include Digital Rights Management (DRM), Healthcare, IoT and decentralized protection of personal data. Table 13 outlines blockchain-based big data use cases for some industry sectors.

Industry sector	Use cases
Health records	Data from healthcare sector comes from a variety of sources (e.g., clinical trials, patient database, diagnostics reports), in a range of streams, with varying frequencies. This "big data" is typically shared among a number of stakeholders and needs to be accessed and interpreted in a time-bound manner. MedRec [60] deploys three types of smart contracts on Ethereum blockchain and structures the large amount of medical records. The first type of contract called Registrar Contract is restricted to certified institutions and stores participants' identity, relevant information, and public keys. The Patient-Provider Relationship Contract is triggered when a node stores or accesses data belonging to another node. Finally, the Summary Contract helps patients to locate their medical history. Other studies resolve interoperability issues in health records, and explores effective use of blockchain and cloud services for healthcare IT and research [61].

[33] Coala IP is blockchain-based, community-driven protocol for IP licensing: https://www.coalaip.org/

Digital Rights Management / Intellectual Property	Maintaining proper rights and being fairly compensated for digital art on the Internet has been a challenging task. Some studies are exploring the use of blockchain in providing proof of ownership by storing time-stamped transactions with hash value of digital art. For example, Ascribe [62] and Monegraph [63] are using bitcoin network to verify the authenticity of artwork online and in real-time. The former focuses on tracking transactions that share and sell digital art, and the latter explores an ecosystem for licensing of digital art. The idea common to both approaches is that the owner possesses the private key and the original copy of the hashed art.
Digital trust for big data	Several studies are exploring how blockchain-based solution can be used to improve privacy in big data. For instance, while [64] provides an approach to access control, [65] studies how users can verifiably control how their personal data is used in social media.
Open data community	The most critical resource required for obtaining high-quality analytics are the datasets. Traditionally, these datasets have been scattered across the web and many datasets are proprietary. The IPDB Foundation is building a global database that simplifies the task of managing other datasets. Any registered user can submit datasets and use other's data. While the data is stored in a decentralized file system such as IPFS, pointer to the data (or meta-data) is stored using Interplanetary Database (IPDB) [66], and datasets are connected using Interledger protocol [21], forming a global resource for data analytics.

Table 13: Big data and blockchain use cases [58] [59]

Architecture: This section provides an overview of BigchainDB [16] since it is one of the first blockchain database projects and a highly notable one. BigchainDB, instead of scaling the blockchain technology, started with a big data distributed database and added blockchain characteristics to it. First, this project conducted preliminary performance tests among existing distributed databases such as Cassandra, HBase, Redis, MongoDB, RethinkDB and ElasticSearch, and compared them over properties like consistency and change notifications, to select RethinkDB[34]. Three main features were then added to RethinkDB: i) decentralized control, ii) immutability, and iii) the ability to create and transfer assets.

BigchainDB presents API to its clients, giving an impression that there is a single blockchain database, while internally there are two distributed databases (RethinkDB): the first database S maintaining an unordered set of transactions and the second database C storing the blockchain. The BigchainDB consensus algorithm (BCA) connects S and C databases. When a new transaction arrives to a receiving node, it is validated, and a valid transaction (according to that node) is stored in S. Identical transactions arriving later are rejected. The receiving node also randomly assigns transactions to one of the other nodes.

There are two types of nodes: signing nodes and non-signing nodes. A signing node, running the BCA, processes the transactions from S as follows. It moves the unordered transactions from S to an ordered list, creates a block of transactions, and records the block in database C. Each block in C is referenced to a parent block and its data, making C a blockchain.

A voting process among signing nodes decides whether a block is valid or not. To this aim, each signing node checks the validity of every transaction in the block; if the block contains at least one invalid transaction, it votes the entire block to be invalid [16]. If all the transactions in the block are valid, it votes as the block to be valid. If a majority of votes is valid, the block is decided to be valid and recorded immutably in the blockchain.

[34] RethinkDB is a JSON (NoSQL) open source database written in C++. It has an active development community and performs well in terms of scalable real-time feeds, which is useful for collaborative applications, connected devices (IoT) and market places, among others. After building the first version of BigchainDB using RethinkDB, the project is working towards other distributed databases (e.g., MongoDB).

2.6.3 Internet of Things (IoT)

Introduction to IoT and current challenges: The Internet of Things (IoT) is an ecosystem consisting of numerous physical objects (things) that are connected via the Internet. This paradigm is bringing more and more things into the digital fold every day and has the potential to advance the automation of every object used in our life. As a result, many organizations are massively investing in IoT-based solutions that can expand and improve business processes and accelerate growth. While the rapid evolution of the IoT market provides a number and variety of IoT solutions, some key challenges need to be addressed to make solutions trustworthy and scalable in performing common tasks such as sensing, processing, storage, and communicating, as listed below [67] [68]:

- **Scalability:** Current IoT platforms are largely based on the centralized server/client model where all things are identified, authenticated and connected through cloud servers that provide huge processing and storage capacities[35]. This architecture creates a bottleneck while scaling IoT solutions to a large number of devices.
- **Security and privacy** concerns become a paramount challenge for individuals, corporations, and governments, considering the huge volume of data collected from millions of devices (including from critical applications such as healthcare).
- **Lack of data standards:** The development of a wide range of IoT solutions, supported by different manufacturers, has resulted in several protocols and application-specific platforms rather than a uniform approach. In this context, interoperability of devices and platforms is a key challenge to the growth of IoT[36].
- **Cost** is a huge barrier for IoT solutions (particularly for the ones following server/client model) with high infrastructure maintenance costs associated with clouds processing and storage, server farms, and networking equipment. These costs are only expected to grow in the future with a larger amount of devices and communications that needs to be handled. Moreover, each of these infrastructure blocks can potentially become a point of failure, disrupting the entire network.
- **Lifecycle management:** The process of configuring and managing numerous devices is a complex process and is a major concern hindering easy movement to IoT paradigm. For instance, from the manufacturer's point of view, the distribution of software updates to millions of devices (sometimes, even a long time after they have been discontinued) incur very high costs.

Blockchain for IoT: The decentralized, autonomous, and trustless capabilities of the blockchain technology can potentially serve as the missing link that can address the challenges in the IoT paradigm. In particular, blockchain can be used for processing of transactions and coordination between devices that enable autonomous functioning of smart devices without the need for the centralized authority. As a result, blockchain opens the door for IoT scenarios that were difficult, or even impossible to implement without it[37]. Note that the use of blockchain within IoT scenario would provide a more resilient ecosystem for devices to operate on, with no single point of failure and with significant savings to IoT industry manufacturers. In fact, several enterprise IoT technologies have already started analyzing the opportunities and challenges in adoption of blockchain technology.

The benefits of adopting blockchain within IoT are illustrated using the following examples [69] [70] [67]:

- **Devices management:** The manufacturer itself can provide the first transaction requesting the update, but once it is propagated to sufficient number of nodes, the manufacture's node can stop this service. Let the smart contract allows devices to share the binary/update they installed; then, a device that joins the network after the manufacturer has stopped supporting this service, can still retrieve this firmware update from one of its peers and be assured about the authenticity of the file received. This automated process hence is significantly simple, efficient and secure as compared to current centralized systems where the device requesting the update to the manufacturer's server gets a 404 error.

[35] https://www.bbvaopenmind.com/en/a-secure-model-of-iot-with-blockchain/

[36] The ISO/IEC JTC 1/SC41 Internet of Things and related technologies is actively developing standards to address this issue.

[37] https://iot.ieee.org/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

- **New billing services:** A blockchain network that supports cryptocurrency tokens provides a billing layer that stimulates marketplace of services between devices. For instance, a node A that provides a copy of the firmware update to node B may charge B for serving it. EtherAPIs is a tool-suite that allows nodes to monetize API calls – in this case, the caller needs to make necessary micropayment (in Bitcoin or Ethereum respectively) to obtain APIs.

Blockchain and IoT use cases: Several start-ups (e.g., Filament [71]) as well as consortiums (e.g., TIoTA) have demonstrated different ways of using blockchains within IoT scenarios (e.g., to automate the end-to-end processes, integrate various business participants). Table 14 presents blockchain-based IoT use cases for different industry contexts.

Industry sector	Use cases
Supply chain [68]	In current supply chains, each stakeholder maintains its own database/ledger. Even when the data is shared with the processes, it is often not sufficiently reliable to trigger concrete actions. Blockchain can help solve some of the key problems in the supply chain: visibility, optimization, and demand. For example, the combination of blockchain and IoT can be used efficiently for tracking food items from farm to packaging and shipping. In this context, IoT can be used to obtain and process location, refrigeration, soil, and weather data streams, and blockchain can make all relevant data available to participants in real time, together identifying contamination and reducing food waste in the supply chain.
Smart home / smart cities [70]	A large number of devices and sensors are being used to monitor and manage cities and buildings, with the goal of providing IoT-enabled technologies that improve operations and experience of residents. A blockchain-enabled IoT system (in this context) can secure devices and the data collected. All stakeholders in the business network can collaborate via a blockchain to provide timely service and to automate payment processes based on quality of service.
Industrial IoT[38] [72]	A recent model in the manufacturing domain consists in using IoT and cloud technologies to enable on-demand access to shared pool of configurable manufacturing resources. However, this model currently requires trusted intermediaries for transactions between users who wish to avail manufacturing services. To address this challenge, a peer-to-peer decentralized platform based on blockchain has been proposed.
Energy and utilities	The use of smart contracts and blockchain technology in the energy sector enables peer-to-peer market where machines can buy and sell energy automatically. In these lines, a set of software and hardware technologies are being developed that enable users to trade solar energy from each other[39]. Realizing the disruptive potential of blockchain for the energy industry, companies are also building mesh networks of smart devices and applications that enable devices to discover, communicate, and interact with each other. This model allows efficient monitoring of energy grids and troubleshooting issues in a timely manner.
Healthcare [69] [61]	The data captured from medical monitoring devices are being stored on blockchains to improve security and privacy and smart contracts are being deployed to implement access control policies that enable participants to read data only if policy rules are satisfied (e.g., approval of 3 or more parties). This model is extended to provide patient records to required participants (e.g., insurance providers) and to automate payments processing based on trustworthy data in real-time.

Table 14: Internet of Things and blockchain use cases [67]

[38] https://slock.it/

[39] Trans Active Grid. http://transactivegrid.net

Architecture: Figure 13 illustrates the typical architecture of an IoT application supported by a blockchain platform (e.g., by the Hyperledger Fabric) [67]. The system consists of three main components: i) IoT devices and gateway, ii) an IoT platform that connects and manages IoT devices as well as analyzes the sensor data, and iii) a blockchain platform. The system developer deploys a smart contract that defines conditions based on device data (e.g., reject a shipment if the temperature – measure by sensors – is beyond a certain threshold) on the blockchain.

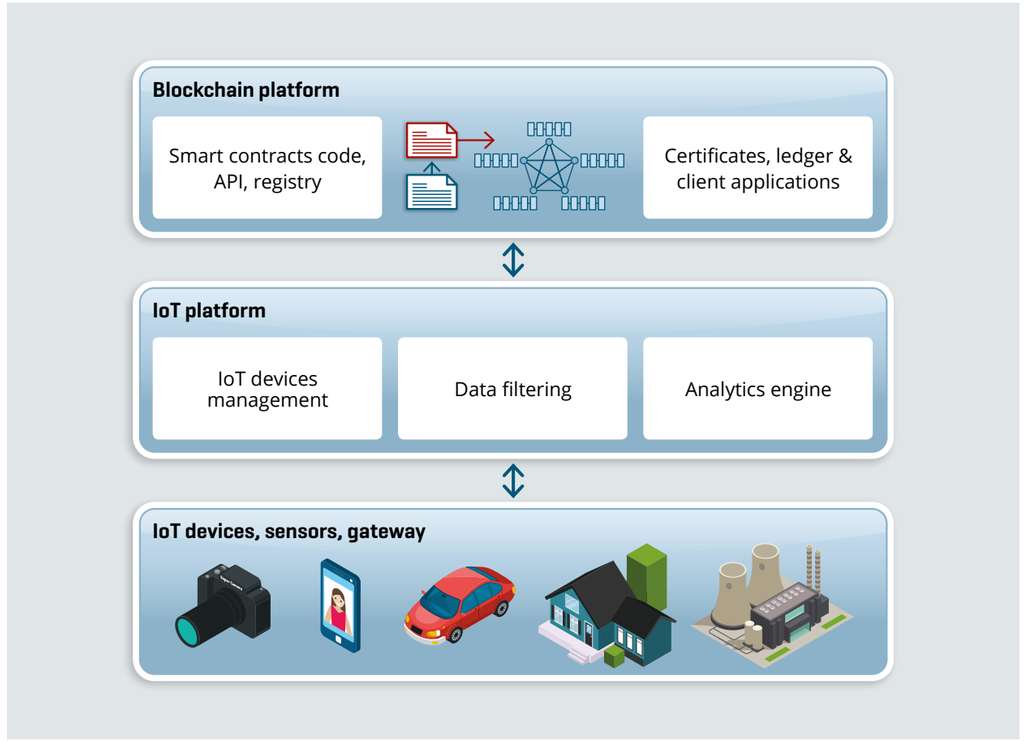


Figure 13: IoT and blockchain (typical) system architecture

The data from (sensors/gateway) devices are sent to the IoT platform which in-turn filters/aggregates and subsequently sends the data to the blockchain. Once the data is received, the smart contract is triggered with appropriate parameters and transactions are recorded on the blockchain. Therefore, the blockchain platform, in case of Hyperledger Fabric as an example, provides [67]:

- A (private) blockchain peer-to-peer network infrastructure;
- Certification authority server that manages the identities of IoT devices;
- Smart contract / chaincode written in Golang. The smart contract developer can provide also an API that allows one to initialize, invoke and query data;
- A ledger that contains all transactions and the world state that denotes the current value of smart contract data.

3

Blockchain and digital trust

3. Blockchain and digital trust

Trust in ICT is essential and is no longer a matter of security alone but transversal to various aspects of hardware and software ranging from consumer devices and equipment to service providers and data centers [73]. Although achieving digital trust is a paramount challenge, it is essential for broad and successful adoption of any technology. This chapter presents the basic components of digital trust namely **security and privacy** in the context of blockchain and distributed ledger technologies. Other relevant topics such as the **relationship** between **blockchain** and **Public Key Infrastructure (PKI)** as well as the EU's General Data Protection Regulation (GDPR) are discussed briefly. Note that other digital trust properties such as interoperability, risk management and usability – although important – are not discussed in this chapter.

3.1 Security

Blockchain and cryptocurrencies in particular are attractive targets for attackers. On the one hand, the technology is still immature and probably hiding several bugs, and on the other hand, the code that interacts with tokens usually have real-world value. In fact, attackers have been successful at a number of tactics, and have aimed at smart contracts, the network itself, cryptocurrency exchanges and wallets, and/or end users.

In this section, first, the security risks that exist in the core operations of blockchain (affecting both blockchain 1.0 and 2.0) are discussed. Then, the risks unique to smart contracts (affecting blockchain 2.0) are introduced with examples of real attacks.

3.1.1 Security risks to core blockchain operations

The blockchain technology is inherently prone to several security risks:

- **51% vulnerability:** The consensus mechanisms such as PoW (see Section 1.5), that establish trust in the system, have 51% vulnerability. If a miner's hashing power is more than 50% of the total hashing power of the blockchain, then that miner could control the entire blockchain [74]. In January 2014, the mining pool ghash.io reached 42% of the total bitcoin computing power. A number of miners voluntarily dropped out of the pool[40] and ghash.io issued a statement that it would avoid reaching the 51% threshold in the future. Similarly, in PoS-based blockchains, 51% attack may occur if the number of coins owned by a single miner is more than 50% of the total blockchain. An attacker successful at 51% attack could launch several other attacks such as [74]:
    1. Initiate double spending attack.
    2. Drop and/or modify the ordering of transactions.
    3. Hinder normal mining operations of other miners.
    4. Impede the confirmation operation of normal transactions.
- **Private key security:** The private key of the user serves as its identity and security credential when using a blockchain. In blockchain applications, the private key is often generated and maintained by the user itself (and not by a trusted third party). If a user's private key is compromised, then the user's blockchain account

[40] https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/

will face the risk of being tampered by the attackers [74]. Since blockchain is decentralized, it is difficult to track attacker's activities – performed using the stolen key – and to recover from the actions performed. Mayer et al. [75] discovered a vulnerability in the Elliptic Curve Digital Signature Algorithm that allows an attacker to compromise user's private key because it does not generate enough randomness during the signature process.

- **Illegal activities:** Users of a public and permissionless blockchain (such as bitcoin) could have multiple addresses and these addresses need not have any relationship with the user's real life identity. This aspect has been exploited to perform illegal activities (e.g., ransomware). Moreover, since users can buy and sell products from third party platforms, and this process largely remains anonymous, it is hard to track user behavior and enforce legal sanctions (e.g., the online marketplace Silk Road has been used for illegal activities [76]).
- **Double spending:** Refers to the scenario where a user spends the same cryptocurrency multiple times for different transactions. In PoW-based blockchains, attackers could exploit the time between two transactions' initiation and confirmation to launch an attack. Such an attack is referred to as a race attack and results in double spending [74]. Before the second transaction is mined to be invalid, the attacker gets the output of the first transaction [77].

3.1.2 Risks due to smart contracts

Vulnerabilities in smart contracts: Consider smart contracts executed in Ethereum for instance. A high-level programming language such as Solidity is used to write a smart contract, which is then compiled to the EVM bytecode (see Section 2.3). In this context, the programmer using Solidity defines sets of functions; however, since EVM does not support functions, the compiler translates each function to a uniquely identifiable signature – based on the function's name and type parameters. At run-time, when a function is invoked, this signature is passed as input to the contract. If the signature matches a specific function, the corresponding code is executed; otherwise, it jumps to the fallback function [25]. The fallback function can be viewed as a special function that can be arbitrarily programmed and that has no name and parameters. This function is also executed when the contract passes an empty signature (e.g., while sending ether to the contract).

This mechanism of contract execution has resulted in multiple vulnerabilities and many of these have been exploited. Based the [25] [74], Table 15 outlines a taxonomy of vulnerabilities in smart contracts, their causes, and the attacks that exploit a given vulnerability (where information is available).

Source	Vulnerability	Brief description and cause	Resultant attack
Contract source code (Solidity)	Call to the unknown	Some primitives in Solidity that are used for invoking functions and transferring ether invoke (as a side effect) the fallback function of the callee/recipient.	The DAO attack [78]
	Out-of-gas send	When using the function send to transfer ether to a contract, an out-of-gas exception might incur.	King of the Ether Throne [79]
	Exception disorder	In Solidity, an exception could raise in various situations. For instance, • When the call stack reaches its limits; • If the execution runs out of gas; • If the command throw is executed. Depending on how contracts call each other, Solidity handles exceptions in different ways, affecting the security of smart contracts. For instance, believing that a transfer of tokens was successful because no exceptions were raised could lead to attacks.	King of the Ether Throne [79], GovernMental [80]
	Reentrancy	The transactions are designed to provide atomicity and sequentiality. These properties usually give an impression to programmers that, when a non-recursive function is invoked, it cannot be re-entered before its termination. However, this is not always the case: the fallback mechanism may allow an attacker to re-enter the caller function. This could result in unexpected behavior, and in loops of invocations that could consume all the gas.	The DAO attack [78]
	Field disclosure	Fields in contracts can be declared as public or private. However, a private field does not guarantee its secrecy because, to set the value of a field, users must send a suitable transaction to miners who in turn publish it on the blockchain. Since the blockchain could be public, everyone can access the contents of the transaction, and infer the value of the field.	Multi-player games [25]
EVM Bytecode	Immutable bugs	A contract published on the blockchain cannot be altered. The drawback of this immutability is that if a contract contains a bug, there is no direct way to patch it.	Rubixi, GovernMental [80]
	Lost Ether	One has to specify the recipient address while sending ether. Many addresses are not associated to any user or contract and there is no direct way to detect such addresses. As a result, ether sent to such addresses are lost forever.	/

Blockchain	Unpredictable state	When a user sends a transaction to the network to invoke a specific contract, there is no assurance that the contract will be run in the same state in which the user sent the transaction. This may happen in various circumstances: ● Other transactions meanwhile change the state of the contract. ● Despite being the first transaction, it may not be the first to be executed. Note that, when miners group transactions into blocks, they are not required to preserve any order. ● In case the blockchain forks. Not knowing the state in which a transaction will be run could result in vulnerabilities. For instance, when invoking contracts that can be dynamically updated, the owner can link this contract to a malicious component that could steal ether.	GovernMental [80], Dynamic libraries [25]
	Randomness	Execution of EVM bytecode is deterministic i.e., under normal behavior, all miners get the same results. To simulate non-deterministic choices, some contracts (e.g. lotteries, games, etc.) generate pseudo-random numbers, where the initialization seed is chosen uniquely for all miners. However, [81] indicates that an adversary could bias the outcome.	/
	Time constraints	Several applications use time constraints to determine which actions are permitted (or mandatory) in the current state. Such time constraints are implemented using block timestamps that are agreed upon by all the miners. All the transactions within a block share the same timestamp and a contract can retrieve this information. This guarantees coherence, but it may also expose a contract to attacks, since the miner who creates the new block can choose the timestamp with a certain degree of arbitrariness. A malicious miner could gain by choosing a suitable timestamp for a block it is mining.	GovernMental [80]

Table 15: Security risks in smart contracts [25] [74]

Under-priced operations: As discussed in Section 2.3, each operation in Ethereum is set to a specific gas value based on its execution time, bandwidth, memory consumption and other parameters. The goal is typically to set the gas value of an operation proportional to the computing resources it consumes; however, some gas values are not set properly [74]. For instance, the gas value of some intensive input-output operations are set too low, allowing attackers to execute these operations in large quantities, thus launching Denial of Service (DoS) attacks on the blockchain.

The operation EXTCODESIZE has been exploited to attack Ethereum [82]. When this operation is executed, it reads the state information and the node reads the hard disk. The gas value of EXTCODESIZE was set at 20; this allowed attackers to call it more than 50,000 times in one transaction, causing consumption of a lot of computing resources. The block synchronization process in turn became significantly slower as compared to the normal situation. Similarly, attackers exploited the under-priced operation SUICIDE to launch DoS attacks [83]. In this attack, SUICIDE was exploited to create about 19 million empty accounts (to be stored in the state tree), wasting hard disk resources. The result of this attack was signification reduction in the node information synchronization and transaction processing speed.

3.1.3 Blockchain and PKI

Public Key Infrastructure (PKI): Public key cryptography consists of a pair of keys (pk,sk), where pk denotes a public key and sk denotes a private key. Revealing the public key does not compromise the private key but the latter needs to be kept secret by its owner. This technique not only allows secure communication over an unsecure public network but also supports verification of the identity of an entity through digital signatures.

A Public Key Infrastructure (PKI) is a system which handles digital certificates, i.e., PKI creates, stores, distributes, revokes and deletes digital signatures. It binds an identity, verified through a registration process, with a public key and issues a certificate delivered and signed by a Certificate Authority (CA). Thus, a certificate contains an identifier, a public key and a digital signature. The purpose of the PKI is to map a public key to its corresponding identity; it also maintains the database of issued and revoked certificates.

Blockchain and PKI: Public Key Infrastructure (PKI) facilitates strong authentication by binding an identity to a public key by means a trusted third party (CA). It serves as a fundamental component in blockchain and distributed ledger systems (see the process of creating and validating transactions in blockchain described in Section 1.1, for instance. Similarly, for a private and permissioned blockchain, digital signatures could be used to pre-select the nodes and to establish trustworthiness in validating and storing transactions in the blockchain.

By complementing blockchain and PKI, the security of ICT could be improved in general. This potential has attracted increasing research attention recently; some promising solutions are discussed here (note that the state-of-the-art is not mature yet).

- **Certcoin** is one of the first **decentralized PKI** based on NameCoin[41], which is a fork of bitcoin and is built to be a decentralized domain name server. The users of certcoin are required to trust that most of the other users are not malicious, instead of trust a third party or a small set of users [84].
- **Emercoin** on the other hand provides an implementation of PKI and Access Control List management called EmcSSH[42].
- Fredriksson [85] proposed a distributed X.509 PKI, backed by a blockchain, by designing a specific account tree and a modified Proof of Stake protocol based on Merkle proofs. Currently, certain properties of the proposal such as the verification of the certificates or their issuance are not well studied. However, the idea of using X.509 PKI remains promising, in particular because of the strong security provided by the blockchain structure, but some research challenges need to be addressed to obtain a full blockchain-based PKI.

For the sake of completeness, Table 16 compares several properties of PKI and public and private blockchains, based on [86].

[41] https://namecoin.org/

[42] https://emercoin.com/

Criterion	PKI	Permissionless blockchain	Permissioned blockchain
Organization	Centralized	Decentralized	Decentralized
Governance	Operating organization	Community	Consortium
Technology	Hierarchical servers	Distributed nodes	Distributed nodes
Trust basis	Trust in the central entity	Consensus mechanism	A combination of trust in the consortium as well as the consensus mechanism
Regulation	Available (e.g., eIDAS)	Very limited but evolving at the moment	Very limited but evolving at the moment
Transparency	Limited	High because of open access and transaction chaining	High transparency due to transaction logging
Maturity	Mature; used widely in real-world applications	Immature	Immature
Reach	Wide spread particularly among enterprises	Limited (and largely constrained with cryptocurrencies)	Proof-of-concepts

Table 16: Comparison between PKI and public and private blockchains [86]

3.2 Privacy

The privacy provided by public and permissionless blockchain is limited to **pseudonymity** since network nodes are identified by their public keys, and transaction details such as the transaction amount, assets being transferred, and metadata including the time of execution are **not confidential** and are available to anyone [7] [87]. This lack of confidentiality is cited as a major concern by 56% of the 134 market participants surveyed by Greenwich Associates [7]. Such concerns arise due to various factors including the privacy requirements enforced by legislation (General Data Protection Regulation – GDPR), regulation (client confidentiality) or contract (commercial confidentiality).

R3 makes the following distinction between the terms **confidentiality** and **privacy** in blockchain [7]:

- **Confidentiality** refers to protecting data (e.g. transaction details, the business logic of smart contracts) from unauthorized third parties.
- **Privacy** refers to protecting the identities of blockchain participants, and parties to transactions, from intrusion.

This definition of confidentiality and privacy implies protection of both data written to the blockchain as well as the identities of the parties involved. This necessitates that [7]:

- The identities of the parties involved in a transaction should not be revealed to an unauthorized third party from the information written to the blockchain, including the metadata.
- Transaction details are not available to unauthorized parties unless one of the counterparties choose to disclose this information.
- Transaction details could not be inferred by collating, analyzing or matching with the information stored off-chain (see Section 3.2.1). This includes the use of graph analysis, pattern matching and machine learning to construct a profile of a counterparty based on the activities associated in the ledger.

Sections 3.2.1--3.2.3 review the technologies and protocols that are emerging as potential solutions for adding confidentiality and privacy to blockchains, and Section 3.2.4 discusses blockchain in the context of the GDPR. At a high-level, individual techniques proposed to improve privacy and confidentiality in blockchain aim to hide either the identity of the sender, or the identity of the receiver, or to hide transaction details. Note that in practice, a combination of these techniques are used to achieve greater degree of confidentiality and privacy. For instance, Zcash[43] combines zero-knowledge proofs and stealth addresses, and Monero[44] uses ring structures, stealth addresses and Pedersen commitments.

3.2.1 Storing sensitive information off-chain

A simple approach to restrict read access consists in configuring the blockchain to be private and permissioned. However, this approach is not suitable for use cases in which participants do not want to share transaction details with others (e.g., competitors within the network). Furthermore, a trusted third party is often required to manage access to the blockchain [7]. This could become a source of additional costs and a potential single point of failure. Finally, any breach of the access control mechanism or information leakage could reveal transaction details stored in the blockchain.

An alternative to restricting read access is to store transaction details "off-chain" – on another system that is configured with access control restrictions. The off-chain database system effectively provides an enterprise-grade restricted read access system. This solution is different from the previous technique is the sense that the blockchain itself can be public and permissionless while the nodes on the blockchain have regulated access to data.

The blockchain stores a hash of the actual transaction details. A node involved in a transaction can verify that its view of the transaction matches with that of the other party's by comparing the hash of the transaction details [7]. The actual transaction details cannot be gained by viewing the blockchain, providing confidentiality of transaction details, while facilitating access to authorized nodes as well. This technique could support use cases where participants may wish to keep details of their bilateral transactions private from other blockchain participants [7].

While this solution is actively being considered by many real-world applications, the following aspects need to taken into account:

- By storing information off-chain, the blockchain may no longer serve as a single, shared source of truth.
- Storing transaction details off-chain could require counterparties to maintain their own records, or delegate that responsibility to a trusted third party. This results in additional costs, potential single point of failure and information leakage.

3.2.2 One-time addresses and stealth addresses

One-time addresses: If a node in the network uses the same address to perform all transactions, an attacker can observe the transactions and infer sensitive information (e.g., the identities of the parties involved). A solution proposed to solve this problem consists in leveraging a one-time address for each transaction – i.e., the receiving party generates a new address and communicates it to the sender, who in turn uses this address while performing the next transaction. Since the new address has no transaction history, it is difficult for an attacker to observe and assemble a clear view of transactions flow.

[43] https://z.cash/

[44] https://github.com/monero-project/monero

Since a certain one-time address is used in a receive and then in a send transaction, additional addresses become associated, and can be used to de-anonymize transactions. For instance, let X be a one-time address; if Alice has sent to X and X has sent to Bob (X being the one-time address), then an attacker could use the graph analysis technique to infer that X is related to both Alice and Bob [7]. Given that information leakage concerning the identity of the receiver does not occur until it is involved in another transaction as a sender, one-time addresses may be suitable for use cases where counterparties only want to keep their involvement in a transaction private for a limited amount of time. Note that this technique aims to hide only the identity of the counterparties; the transaction details are published on the blockchain.

Stealth addresses: In contrast to the above solution, the technique called stealth addresses allows the sender to generate the one-time addresses. Here, the recipient generates a parent key pair and publishes the public key (the stealth address). A sender can then use the stealth address to generate a new one-time address. The recipient uses the parent private key to calculate the one-time address's secret key, which is required to future transaction [7]. This approach significantly reduces the complexity of the one-time addresses technique.

3.2.3 Mixing and coinjoin

Mixing: Another technique that prevents against graph analysis is mixing. Consider transactions exchanging ether as an example: a mixing service receives ether from many nodes, shuffles them, and sends to appropriate recipients but at different times and by splitting it into different amounts. By doing so, the mixing service makes it difficult to trace the flow of funds. In general, mixing services are third party services that take custody of many users' coins for a period but any wallet or exchange could effectively become a mixer. A large number of transactions and a long duration to hold the coins are typically required for the mixing services to be effective.

The mixing technique introduces several risks that must to be taken into account [7]:

- The mixer can steal the coins, or it can be hacked, while holding the coins of its clients.
- Given that the mixer knows the recipient of a transaction, sensitive information could be revealed if the mixer's logs are compromised.
- The mixer could leak the information pertaining the parsing of transactions.
- The mixers are typically anonymous, so the user has no recourse if the mixer has been compromised.

Coinjoin: Coinjoin is a mixing technique that aims to remove the need for a third party and the trust that needs to be placed on it based on the observation that a single transaction can have multiple inputs and multiple outputs. For instance, consider that two parties A and B want to send a bitcoin to parties C and D respectively. Coinjoin creates a transaction combining both sends (i.e., having two inputs A and B and two outputs C and D), where the order of inputs and outputs is randomized. If multiple transactions are combined into one coinjoin transaction, then the uncertainty of the source and the destination of the transaction is higher.

In contrast to the mixing services, coinjoin does not require a trusted third party but all parties involved in a transaction must communicate with each other to sign the coinjoin transaction [7]. This coordination could have drawbacks. First, if there are not enough parties that want to participate in a coinjoin at a given point, this technique could become ineffective. Second, the participants in a coinjoin could infer how to unmix transactions and know all other participating parties.

3.2.4 Blockchain and GDPR

The European Union has defined the General Data Protection Regulation (GDPR) to pursue the goals of data protection and the free movement of personal data in the internal market.

Scope of GDPR: The regulation applies to 'personal data' defined as "any information relating to an identified or identifiable natural person" – the 'data subject'. An 'identifiable person' is defined as a natural person who "can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that natural person".

Completely anonymous data does not amount to personal data and falls outside the scope of the regulation. However, pseudonymous data qualifies as personal data because indirect identification of a natural personal remains possible.

Applying GDPR to blockchain: As discussed above, two sets of data are stored on blockchains: transactional data stored in the blocks and public keys. The former could directly comprise personal data and the latter is pseudonymous. Table 17 analyzes whether data subjects can invoke their rights with data controllers (nodes maintaining the database) in a blockchain environment based on [88]. This analysis is restricted to substantive rights, and is provided to stimulate a better understanding – GDPR clauses considered here are representational and not exhaustive.

From a legal point of view, a data subject can invoke rights vis-à-vis every single node in the network. However, from a technological point of view, it is unclear how nodes could implement related requests to update, delete or restrict data. In addition to these technological challenges, regulation's procedural obligations also need to be considered in the context of a blockchain system.

Data protection right mandated by the GDPR	Analysis of 'data subject' rights on blockchain
Data minimization	The GDPR mandates that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". On the one hand, blockchain is an immutable database that is ever growing, and on the other hand, it is distributed across multiple nodes in the network. These properties pose difficulties in implementing data minimization. Transactional data stored off-chain could be minimized according to the legal requirements circumventing the blockchain. However, public keys cannot be removed retroactively from the ledger.
The right to amendment	The GDPR requires that personal data be accurate and up to date. If this is not the case, "every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay". Moreover, Article 16 GDPR includes the right to obtain rectification from the controller without undue delay. A data subject could therefore address any or all nodes with a request to rectify personal data. Two issues arise in this context: • A data subject cannot identify any or all blockchain nodes that are storing data. • Even if the data subject succeeds in addressing a claim under Article 16 GDPR, nodes may not be able to change any of the encrypted data stored in a block (due to immutability).
The right to be forgotten	Article 17 GDPR mandates that the data subject shall have the right to obtain from the controller "the erasure of personal data concerning him or her without undue delay". Immutability of records is one of the most valuable features of blockchain. However, this very feature makes it challenging to implement Article 17 of GDPR.
The right to access	Controllers typically do not know which data is stored on the blockchain because they often only handle data in encrypted or hashed formats. This data management model poses several challenges from GDPR's 'right to access' point of view: • Article 15 GDPR indicates that a data subject has the right to obtain confirmation from the controller whether or not her personal data is being processed. If a data subject contacts a (controller) node, the latter would not be able to verify whether personal data is being processed. One solution could be that the data subject joins a permissionless network and obtains a copy of all data; however, it is clear whether such a solution would be regarded as a satisfactory solution. • Article 15(2) GDPR specifies that data subjects are entitled to be informed about safeguards where data is transferred to third countries. In the context of blockchains, given that a node validating a block in the EU could thereafter share that information with all other nodes, irrespective of their geographical location. • Article 15(3) GDPR entitles data subjects to obtain a copy of their personal data undergoing processing from controllers, which would be impossible given that the data is cryptographically pseudonymized.

Table 17: Analysis of GDPR data subject rights in the context of blockchain [88]

4

Economic impact analysis

4. Economic impact analysis

Blockchain and distributed ledger technologies are foundational to various forms of commerce such as record keeping, contracting, clearing and settling. Their adoption is expected to reduce transaction costs, streamline operational processes, improve profit margins, and change the roles of businesses within value chains. To understand the benefits and potential risks, organizations across the world are experimenting with these technologies and most initiatives are currently in the banking, financial services, and insurance industries. The top three geographical regions in terms of blockchain-related initiatives are EMEA (40%), Asia/Pacific (30%) and North America (23%), with the U.S. as the country with the most Proof-of-Concepts [89]. The goal of this chapter is to provide an in-depth analysis of the impact of blockchain on businesses, society and the economy at large.

4.1 Economic analysis (high-level view)

Given the rapid advancements in the technology [90], recent adoption by industries [91] and potential influence across multiple economic sectors, assessing the medium to long-term economic impact of blockchain largely remains an open problem [92] [93]. Nevertheless, studies conducted by various organizations expect blockchain (and DLT) to grow rapidly in the near future and its adoption to leapfrog in various economic sectors. Some indicators are listed here as examples to put things into context:

- The World Economic Forum expects that by 2025, around 10% of the world's Gross Domestic Product (GDP) will originate from blockchain-based systems [94].
- Global Opportunity Report [95] estimates blockchain and DLT to grow from $210 million in 2016 to $2.3 billion by 2021, with an annual growth rate of 61.5%.
- The survey conducted by PwC [96] indicates that 77% financial institutions expect to adopt blockchain as part of an in-production system or process by 2020.

Table 18 maps blockchain properties to potential impact on commercial, societal and administration activities, the expected scope of this impact, and example use cases. The potential to exchange value (tokens, cryptocurrencies) in a **decentralized** manner between parties that need not **trust** each other has **transformed the notion of money** and led to a wide range of innovation. This paradigm – if realized at a large scale – could disrupt existing financial, banking and payment infrastructures, thus influencing the economy as a whole. Cheaper and faster remittance, funds distribution and crowd funding of start-ups are examples of use cases representing this paradigm.

Blockchain feature	Tokens/ cryptocurrencies	Secure data registry	Smart contracts
Potential impact on the society, public and private sectors	Transformed notion of: • Money • Trust • Transactions	• Improve traceability, governance and transparency • Reduce the scope for frauds	• New ways of enforcing agreements • Changes in operational processes • Evolution in legal methods
Expected scope of impact	Economy at large	Individual businesses, governance models and public services	Business networks and ecosystems
Example use cases	Payments and remittance; Raising capital; Banking; and Financial services.	Land rights; Identity management; Educational credentials; Health records; IP ownership; Agriculture & food; and Manufacturing.	Supply chain management; Financial services; Energy exchange; Retail; Smart cities; and Art market.
Discussed in	**Section 4.1.1**	**Section 4.1.2**	**Section 4.1.3**

Table 18: Blockchain features vs potential economic, business and societal impact

Since data stored in a blockchain has chronological ordering and the database structure remains distributed, tamper-resistant and immutable, **provenance of information** becomes simple and trustworthy. This is specifically desirable for applications where **transparency, auditability and traceability** are important. Consider land registry as an example: when a piece of land needs to be registered – if relevant data is recorded in blockchain once it is verified to be a truthful entry by the authorities, the landowner can easily provide the proof of his/her rights when necessary. Similarly, the use of blockchain in recording health data, educational credentials, identity documents, IP ownership etc. is being explored and is creating opportunities for various economic sectors as well as improving governance.

Smart contracts allow written agreements to be translated into code that can self-verify if conditions have met to execute the contract as well as self-execute certain actions such as releasing payment and other types of information. Given that the conditions encoded within a smart contract not only involve financial information but also real-world entities, they are being deployed on blockchains to study a wide range of applications including in supply chain management, retail, energy exchange, smart cities etc. Smart contracts cover activities of various entities within a business network and hence is the expected scope of their direct influence (see Section 1.6).

The rest of this section provides detailed economic and business impact analysis of the three above-discussed aspects. The impact of the combination of these aspects (blockchain tokens, secure data registry features, and smart contracts) is then analyzed holistically considering funds distribution, logistics and supply chain management, and digital identity and data protection services as case studies (see Sections 4.2, 4.3, and 4.4 respectively). The analysis for each case study comprises the following set of information.

Figure 14: Aspects studied for each case study

4.1.1 The new notion of money, trust and transactions

The world of money and finance is rapidly transforming thanks to digitized assets and innovative financial channels. This transformation has accelerated with the advent of bitcoin as the first fully decentralized digital currency, and a wide-range of cryptocurrencies derived from it, creating new paradigms for financial transactions and instruments for forging alternative conduits of capital.

Today, more than 1500 cryptocurrencies with market value are being traded[45]. The overall market is highly dynamic because hundreds of cryptocurrencies are being introduced annually and several being disbanded. Nevertheless, in the recent past, cryptocurrencies have received significant funding and support from established institutions and other venture capital (VC) firms. The following insights and figures illustrate the scale of cryptocurrency adoption as well as economic and innovation activities in this area:

- **Public blockchain**
  - The aggregate market cap (market price times number of existing currency units – Figure 15) of cryptocurrencies surpassed $600 billion in Q4 2017 [97].
  - Altcoins[46] and cryptocurrencies such as ether, ripple and litecoin are gaining dominant position in terms of market cap share. While bitcoin accounted for 86% of market cap share at the beginning of 2015, it accounts only for 40% of total market cap share, as on 20th February 2018 [97] (see Figure 16).
- **Enterprise blockchain**
  - The compound annual growth rate for enterprise blockchain is estimated to be 26.2% [98]. This implies that the revenue for enterprise blockchain is expected to increase from $2.5 billion in 2016 to $19.9 billion in 2025 worldwide.

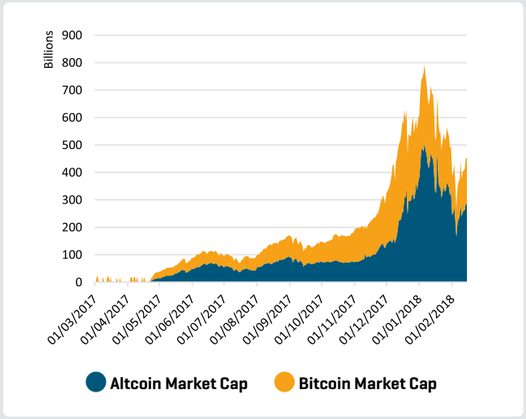


Figure 15: Cryptocurrency market cap (bitcoin vs altcoin) [97]

[45] https://coinmarketcap.com/all/views/all/

[46] The cryptocurrencies that are derived from bitcoin (e.g., by changing parameters such as currency supply, issuance scheme etc.), with little innovation, and are referred to as altcoins.

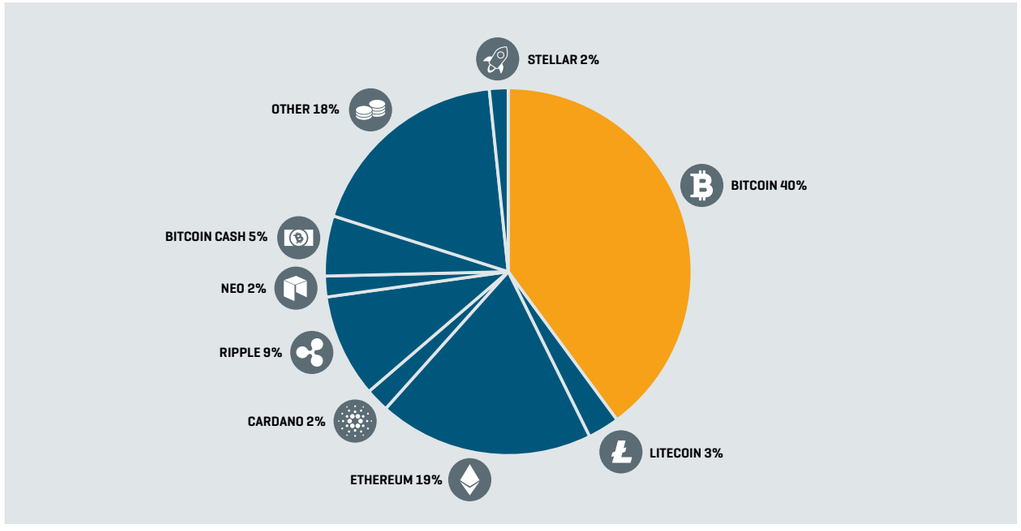


Figure 16: Cryptocurrency market cap (% share) [97]

Cryptocurrency **exchanges** provide platforms to buy and sell cryptocurrencies for fiat currencies or other cryptocurrencies. Figure 17 shows the market share of various exchanges that are serving as platforms for trading, price discovery and liquidity[47]:

- In April 2016, Luxembourg granted a license to Bitstamp to be a regulated cryptocurrency exchange. This license allows Bitstamp to do business in all EU member states as a payment institution.
- Japan-based bitFlyer (which expanded to the US in 2017) became another exchange licensed by Luxembourg as a payment institution in January 2018.
- Bitstamp and bitFlyer together held 25% of market share as on 20th February 2018 (see Figure 17).

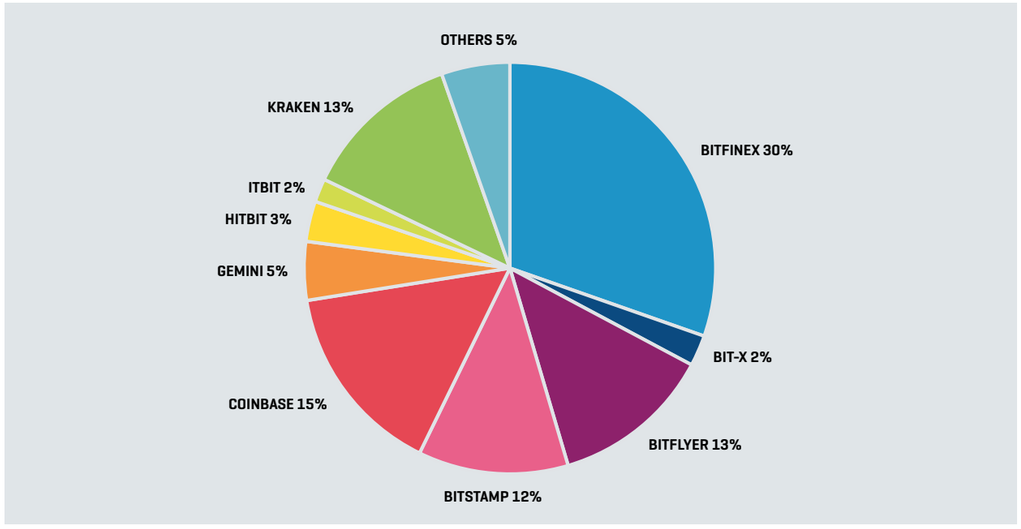


Figure 17: %Market share of cryptocurrency exchanges (Source: data.bitcoinity.org)

[47] Sourced from data.bitcoinity.org on 20th February 2018

The above economic indicators clearly suggest that cryptocurrencies are gaining increasing popularity and are driving innovation towards new notions of money and financial transactions (e.g., transfer of value by sending digital tokens from one account to another without the need of a trusted third party). This paradigm has the potential to create an entirely new set of businesses, jobs and vocabulary in financial services as well as the economy at large. To understand this impact clearly, the rest of this section provides details on the transformed avenues of economy using the following examples: conduits for raising capital, banking infrastructure, payment systems and e-commerce. An extensive case study on the potential impact of blockchain on **funds distribution** is then presented in Section 4.2.

Raising capital – crowd funding and Initial Coin Offering (ICO): A pre-eminent innovation of blockchain technology and cryptocurrencies consists in the way organizations are attracting funding. An ICO, also known as a token sale, is an event in which an organization sells digital tokens[48] for the purpose of obtaining public capital to fund software development, business operations, business development, community management, or other initiatives [52].

During an ICO, token buyers generally contribute fiat currency (e.g., USD) or cryptocurrency (such as ether or bitcoin) to a specified cryptographically generated address. In exchange, buyers receive certain number of the organization's native tokens [52]. In a public sale, anybody who has the capacity to purchase, transmit, and store cryptocurrencies can be a token buyer. Buyers may have a diverse set of motivations: some may wish to use the token primarily for its underlying utility, while others may be speculators who hope to profit from trading gains.

Table 19 illustrates the benefits and risks of ICO based on [52]. Note that regulators around the world are monitoring this phenomenon and several national authorities are issuing guidelines for investors and are expressing concerns and associated risks. CSSF has also issued notices on ICO[49] and virtual currencies[50]. It is important for investors as well as for companies seeking to raise capital to consider such regulatory aspects.

In 2017, organizations raised over $5.3 billion through ICOs, signaling a remarkable tipping point. Among these organizations, Filecoin ($262 million), Tezos ($232 million), Sirin Labs ($157.9 million) and Bancor ($153 million) attracted largest amounts of funds through ICO [99]. Figure 18 and Figure 19 illustrate blockchain funding raised via ICO as compared to VC – highlighting that projects are receiving significant funding and that cumulative ICO far exceeds cumulative VC.

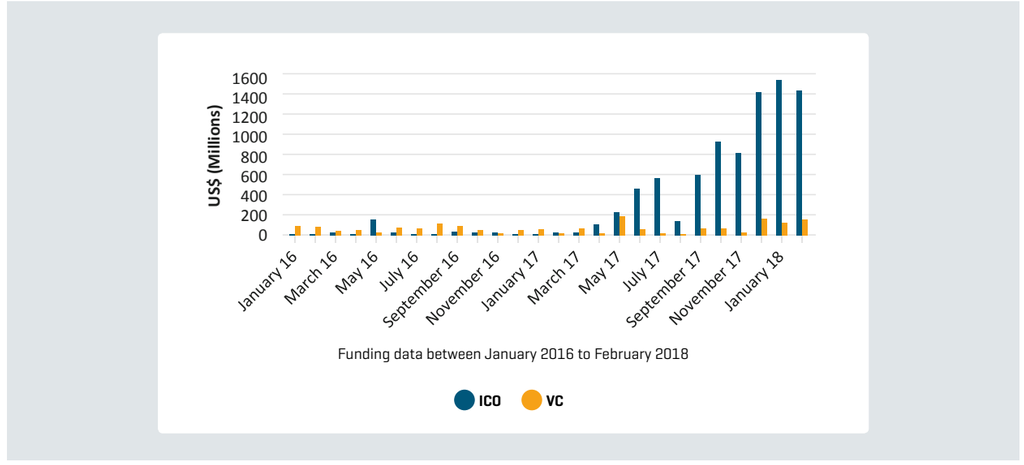


Figure 18: Monthly blockchain funding (ICO vs VC); data sourced from [99]

[48] In this context, a token is a cryptographically secured digital representation of a set of rights. This could include the right to use of a network or software application, right to a share of future earnings, the right to vote on decisions made by the organization etc

[49] http://www.cssf.lu/fileadmin/files/Protection_consommateurs/Avertissements/A_ICOS_140318.pdf

[50] http://www.cssf.lu/fileadmin/files/Protection_consommateurs/Avertissements/A_monnaies_virtuelles_140318.pdf

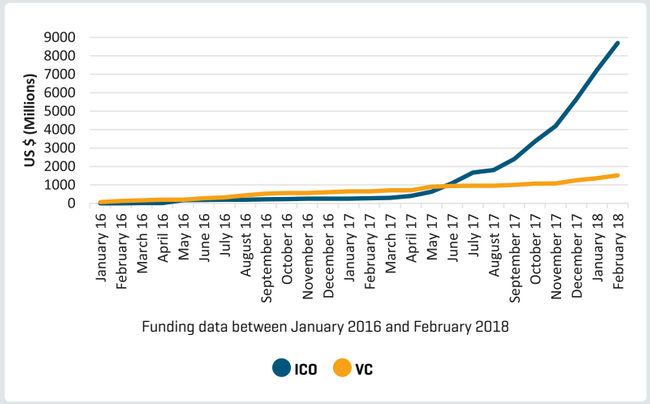


Figure 19: Cumulative blockchain funding (ICO vs VC); data sourced from [99]

Benefits of ICOs	Risks of ICOs
For organizations that issue tokens • A built-in customer base and positive network effects • A new model of financing for open-source projects (including early stage innovations) • Global and non-discriminatory investor/donor outreach • Fast and easy fundraising mechanism • A warm reception from retail investors For investors and donors • Easily transferable • Liquidity • The network effect of value creation • Democratizing investment • Potential for gains	Consumer protection • Lack of due diligence • Smart contracts may have vulnerabilities which permit unexpected transfers • Uncertain basis for token valuation • Education • Unsophisticated token consumers may not be able to maintain or secure keys • Phishing scams Market risks • High price volatility • Market movements attributed to ICO cash outs • Market manipulation • Network lag during large ICOs • Token distribution mechanisms Regulatory compliance • Anonymous or pseudonymous token buyers • Tax evasion • Uncertain regulatory schema • Potential money laundering

Table 19: Benefits and risks of ICO [52]

Banking: Central banks across the world are analyzing the potential benefits and downsides of cryptocurrencies. While some central banks are exploring how cryptocurrencies could improve the accessibility, resiliency and efficiency of monetary and financial transactions, others are studying the changes to be made to existing financial infrastructures [100] [4].

Bank of England published a staff working paper in 2016 presenting a detailed analysis of the macro-economic consequences of a central bank issued digital currency [4]. In their model, a central bank digital currency (CBDC) is a universal, electronic, 24x7, national-currency-denominated and interest-bearing access to a central bank's balance sheet. The macro-economic modifications needed to introduce this model (economic mechanisms such as interest rates, liquidity and monetary policies) are kept to a minimum and privately created cryptocurrencies are not taken into account.

The model builds on an economy with a single, government-defined unit of account and cryptocurrencies are in the form of bank deposits that maintain a 1-to-1 exchange rate with government money. So, the CBDC issuance mechanism makes sure the central bank only trades CBDC against government debt instruments. They show that **CBDC issuance amounting to 30% of Gross Domestic Product** (GDP) would lead to an **increase of almost 3% of the GDP** due to reductions in interest rates, taxes, and monetary transaction costs.

Barrdear and Kumhof (Bank of England) [4] discuss transition risks that need to be managed to ensure financial stability. Policymakers must carry out thoroughly a due diligence before deciding on the transition to a CBDC regime because of the lack of any experience in this new monetary and financial environment. In conventional financial systems, money is propagated from a central bank, through commercial banks, to businesses and individuals. However, if central banks will issue cryptocurrency themselves, the ledgers of central banks and end-users could be connected directly (see Figure 20) [101].

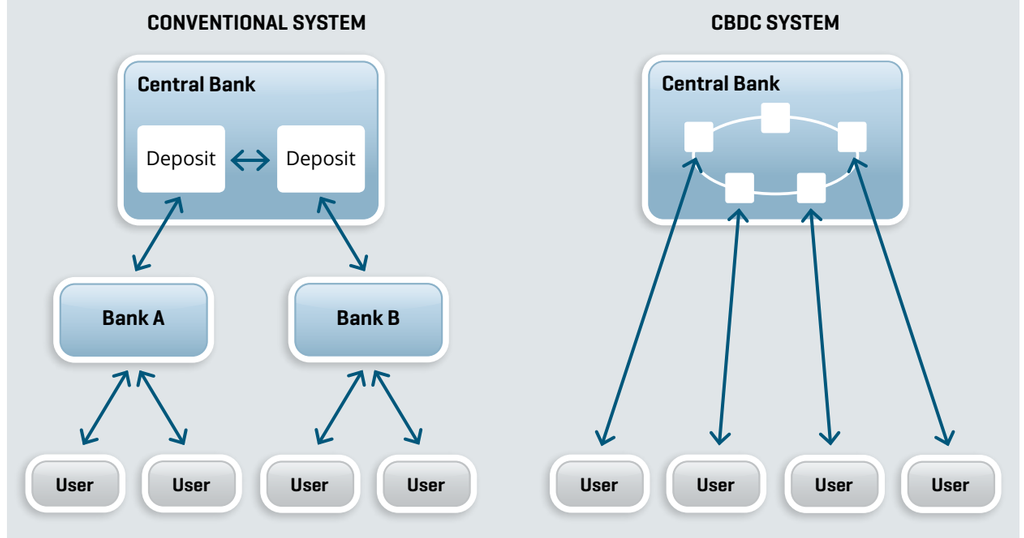


Figure 20: End-users can directly access central bank ledgers [101]

Payment systems: The transformed financial/banking infrastructure (see Figure 20) has the potential to reduce transaction costs and time for making payments. Currently, the average cost to the final customer (sender) is estimated to be 7.68% of the amount transferred; in contrast, using cryptocurrencies and blockchain based platforms, transaction fees is estimated to be around 0.05% of the value of transactions [4].

On one hand, the non-bank transactions are reaching up to 10% of the total payments volume [102], and on the other hand, the global payments volume is increasing approximately at the rate of 5% per year worldwide and is estimated to have reached $601 billion in 2016 [103]. Given these transaction volumes and transformed financial infrastructure, Bitpesa (a blockchain-based payments platform) expects reduction in the costs of international transfers by 75% and the average time of settlement from 12 days to approximately 12 hours[51].

However, for such a payment system to be a real alternative to existing interbank payment systems, the blockchain technology has to make significant progress. For instance, currently it is not possible to process a vast amount of transactions per second at a global scale using blockchain. Similarly, security issues need to be addressed sufficiently (see Chapter 3).

Retail: Another innovation derived from the above-described payment systems consists in blockchain based online shopping platforms that connect buyers and sellers directly. An example is OpenBazaar [104], an online fully decentralized marketplace that runs a peer-to-peer network. It allows anyone to join the network where buyers can purchase goods using a variety of over 50+ cryptocurrencies and sellers are paid in Bitcoin. One only reveals the chosen personal information and transactions are immutable. Currently, OpenBazaar has over 400,000 downloads, 300 merchants and 10,000 listings [105].

4.1.2 Improved governance, traceability and transparency (secure data registry)

The previous section discussed about the influence of cryptocurrencies and blockchain on the economy at large (e.g., restructuring of banking infrastructures and payment methods). This section analyzes the ability of blockchain to ensure integrity, nonrepudiation and immutability of records, and its impact on businesses. Existing literature suggests that these blockchain features could be used for secure exchange of data (e.g., legally binding documents, personal health records), which could help in reducing frauds and improving transparency and traceability, thus transforming existing economic, legal and social systems [106]. In the following, examples across economic sectors are used to understand these opportunities in detail.

Agriculture and food: Blockchain could be used to enhance the traceability and reduce food-fraud by recording validated information concerning the origin and the state of the food. On one hand, all parties in the value chain (farmers, suppliers, processors, distributors, retailers, consumers and regulators) can access real-time information about the food product (e.g., to trace contaminated goods to its source, verify that food is produced without child labor etc.). On the other hand, users will be able to trace-back the entire product lifecycle from the farm to a retailer. A test conducted by Walmart to trace mangoes took 6 days before using blockchain and took 2.2 seconds by using blockchain [107].

The Food and Agricultural Organization (FAO) of the United Nations also recommends use of blockchain technology as a vital e-agricultural infrastructure component for building innovative food systems, and for increasing food safety, security and market efficiencies [108].

In addition to food supply, other blockchain applications in logistics include the fields of flowers, wine, automobile, art, trade finance and pharmaceuticals, to name a few. Section 4.3 provides a detailed **case study** on the impact of blockchain within **supply chain management**.

[51] https://news.bitcoin.com/bitpesa-ceo-claims-bitcoin-based-remittance-companies-have-reduced-costs-by-75/

Public services: Several government organizations across the globe are investing in the blockchain technology to reduce innovation roadblocks and to streamline information across organizations. Potential applications include citizen's identity management, provenance of land/assets and sharing health records securely according to specific rules. The Estonian government for instance is experimenting with distributed ledger technologies to allow citizens to verify the integrity of their records on government databases [109] [110]. Dubai also envisions issuing all government documents on blockchain by 2020 [111].

Currently identity systems that are required to make use of governmental services are state owned. However, digital identities can be recorded in a blockchain and individuals can add things to that identity. Ultimately, an individual would be able to control his/her identity attributes to realize the concept of self-sovereign identity. uPort [112] is an example of a self-sovereign identity system that is built on Ethereum. An individual can then distribute identity attributes for KYC/AML procedures, to pay taxes, and so on.

Furthermore, digital identities could be used to secure e-voting since elections require authentication of voters' identity. Blockchain could be used for casting, tracking, and counting votes based on tamper proof identities. This paradigm could not only reduce voter-fraud, lost records and foul play because of hard-to-falsify records, but also allow voters to verify that no votes were changed, removed or illegitimate added. In 2016, Colombian expatriates successfully experienced the potential of blockchain technology in a plebiscite on whether to approve a peace treaty, as they were unable to vote through the official process [113].

Section 4.4 provides a detailed **case study** on the use of blockchain and DLT for **digital identity management and data protection**.

Manufacturing: Industry 4.0 denotes an integrated manufacturing model that uses several technologies including IoT, cloud computing, artificial intelligence, 3D printing and cyber-physical systems. Blockchain could become a core part of Industry 4.0 by serving as a record-keeper for all the transactions of smart devices. Similarly, 3D printing is moving manufacturing closer to end-users. However, 3D printing vendors still need conventional file-sharing methodologies to sell their wares with a considerable risk of intellectual property theft. Blockchain could provide an audit trail enabling users to track and trace the state of the 3D model file, which might help in protecting intellectual property rights.

Human Resources: The potential to use blockchain as an immutable source of information could create opportunities in streamlining human resources tasks. Consider for instance that an educational institution enters training or graduation data on blockchain. When a candidate applies for a job, the prospective employer could then verify the candidate's educational credentials by accessing the information stored on blockchain. This process of conducting background checks and disclosure of fraudulent claims could be automated and be made trustworthy.

4.1.3 Enforcing agreements

In contrast to cryptocurrencies, smart contracts could be used for complex transactions involving digital assets such as the Intellectual Property Rights (IPR). Smart contracts autonomously change the status of digital assets when predefined rules and conditions are satisfied, triggering relevant execution, enforcement, and payments. The combination of smart contracts and blockchain has the potential to transform the roles of agencies, reduce coordination costs, and consequently revolutionize business networks/ecosystems [114] [115].

Energy: Blockchain provides opportunities to rethink the energy-exchange processes. Traditionally, to gain access to electricity, one goes to an established power holding company or use a re-seller that buys from the big electricity companies. A proof of concept peer-to-peer electricity exchange allows people who own solar panels to sell their surplus electricity at pre-agreed price by means of smart contracts to others in the neighborhood [101]. This innovation, when applied to developing countries, could unlock new modes for delivering sustainable development. The Energy Web Foundation (see Section 2.5) is a global non-profit organization focused on accelerating blockchain technology across the energy sector.

Intellectual property rights: Blockchain could provide a new approach to the creators of intellectual property and change the way they store and share their content (see Section 2.6.2) [116]. For instance, using blockchain technology in the music industry could allow artists to control their musical work (digital assets), extend ownership of their works, and receive payments instantaneously. In other words, licensing agreements could be implemented as smart contracts (to a large extent) and royalties could be transferred directly to the producers, writers, and technicians involved in a song's production.

Legal: Wills provide another good use case for blockchain smart contracts based solutions. Blockchain applications can make the verification of the death of an individual, the authenticity of a will and resolution of will-related litigations easier. It provides verifiable transaction data, identifies correct and complete information and dismisses claims that are without any merit [117]. The **ISO/TC307** has initiated a project on **legally binding smart contracts** (see Chapter 5).

4.2 Case study 1 – Funds distribution

Funds distribution refers to the sale of investment funds to investors through channels such as intermediaries including Independent Financial Advisers (IFAs), banks, asset managers and other service providers [118]. An investment fund in this context is a general term for any investment vehicle that pools together the money of a number of investors and invests in certain markets and securities according to its investment strategy and objectives [118].

Funds distributed exclusively in domestic markets benefit from the existence of established financial infrastructure (e.g., central securities depositories) [119]. Although a unique set of regulations further simplifies their distribution processes, they do not achieve the scale required to generate cost efficiencies due to limited market footprints. In contrast, international funds distributed across multiple domiciles do not benefit from a single infrastructure. A mixture of bilateral links, aggregator platforms, and processing service providers prevail [118]. Documents and data dissemination is channeled through multiple information distributors or resellers. Local notifications must meet various national constraints, including language translation and specific tax reporting duties. Despite being complex, the setup of distribution networks across multiple countries benefits from the economies of scale and costs mutualization [119], and supports the growth of these international funds. Luxembourg has the highest share (63.6%) of authorizations for cross-border distribution in the world and €4.1 trillion net assets were under management in Luxembourg investment funds at the end of November 2017 [118].

4.2.1 Typical business model

This section first presents a highly simplified funds distribution value chain to create a general understanding. In this value chain, an IFA denotes an expert who advises individuals (investors) on their investments. IFA determines individual's financial means, investment profile and goals, and recommends investments that fit their needs. Based on the recommendations made by the IFA, when an investor decides to invest in certain funds, the transfer agent (TA) undertakes the administration of subscriptions to and redemptions from funds. In Europe, banks and insurers are the main distribution channels for retail investors.

Funds administration involves various duties such as the calculation of the Net Asset Value (NAV), proper accounting and the recording of the issue and redemption of fund shares. A regulated institution such as a bank then provides safekeeping of the fund's assets in accordance with the applicable regulations. This institution is commonly referred as the custodian [118]. Intermediaries (e.g., bank, IFA) are typically remunerated either by charging the investor on top of the fund management fee or by charging the fund as a portion of the management or distribution fee.

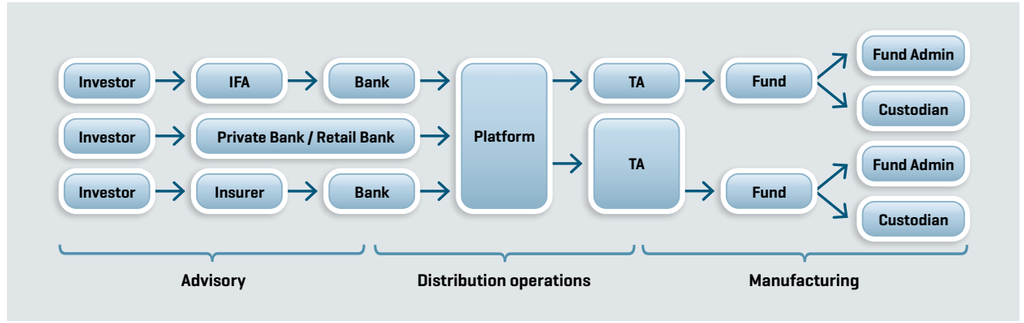


Figure 21: Simplified view of the funds distribution value chain

In reality, funds distribution involves various other market players (e.g., asset managers, distributors, regulators) and activities (e.g., portfolio management, risk management, compliance and due diligence), making the overall domain highly complex with several operational processes as part of daily business. As an example, a breakdown of major operational processes within the fund distribution (and associated management service's) value chain is given in Table 20 [119].

Fund processing	Cash processing	Errors and reconciliations	Compliance and record keeping
• Fund data management • Technology setup and maintenance • Management of dealing channels • Orders management • Client support • Corporate actions • Transfers • Commission payments	• Settlement instruction management • Payment processing • Management of multiple settle models • Dividends payment	• Cash reconciliation • Order reconciliation • Position reconciliation • Error corrections and repairs	• Know Your Customer (KYC) documentation • Compliance verification • Documentation gathering • Account opening and maintenance • Distributor due diligence

Table 20: Activities performed within each operational process (example) [119]

4.2.2 Industry challenges

The trend towards an increasing number of intermediaries has expanded the distribution network, services, as well as the value chain. It has also led to a counterproductive effect of increased costs for asset managers to distribute funds and increased costs for investors to buy funds. Moreover, the profit margins of intermediaries such as transfer agents (TAs) are reducing due to their operational models and/or size. For instance:

- TA services are being offered for free under packaged propositions with fund custody.
- TA services are seeing diminishing turnovers due to increased intermediation that reduces de facto number of accounts and transactions (traditionally their main sources of revenue).

Hence, across the industry on one hand there is a need for consolidation to gain critical mass and profitability and on the other hand a need for delivering added-value solutions to be more attractive. Creating added-value solutions is difficult because funds are currently distributed to investors largely via intermediaries and the fund/asset managers do have all information about investors' requirements.

Figure 22 highlights major challenges faced by the industry – in four categories.

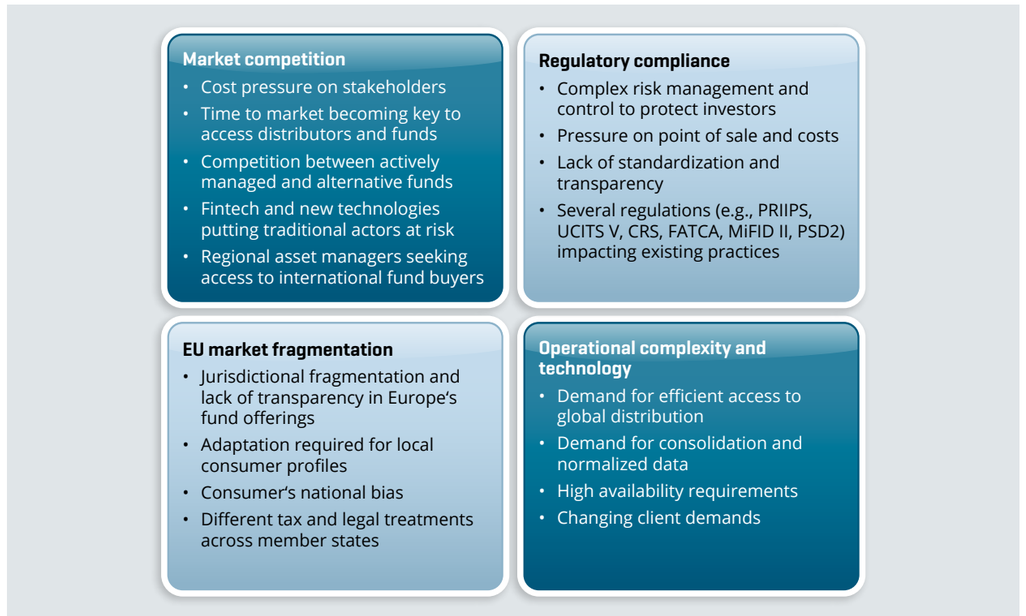


Figure 22: High-level view on the challenges within funds distribution (this list is representational and not exhaustive)

As a response, among others, industry has made significant progress in addressing the challenges due to operational complexity (e.g., by automating and speeding operational processes) over the past decade. However, the experience of subscribing to a fund is still not optimal for institutional as well as retail investors. This is primarily because the overall trade lifecycle remains labyrinth with various manual processes and intermediaries, taking several days (up to 4 days [120]) from initiation to settlement. Such challenges relating to operational processes (see Table 20) and associated costs are discussed here in detail, based on [119].

- **Fund processing:**
  - **Orders processing:** Given the continuous effort by the industry to automate order flows, the overall industry level of straight through processing in Luxembourg increased from 47% to 77% in the last 8 years. However, the remaining 23% tasks involving orders processing represent significant costs for the industry. Among these costs, order routing, booking and confirmation of manual orders cost €365 million. The maintenance of bilateral connections (e.g., via SWIFT or proprietary FTP formats), parameterizing share classes, costs due to SWIFT/FTP terminals, and SWIFT messaging cost approximately €80 million. Hence, the total cost of processing orders is estimated to be €450 million per year in Luxembourg.
  - **Transfers, corporate actions and dividends:** In addition to orders processing, the funds distribution process involves other activities such as transfers, dividends and corporate actions handling. These activities are largely performed manually. For instance, stock transfers comprise 10% of subscription and redemption volumes but the amount of automation at transfer agents and distributors is well below the ones for orders processing. Consequently, the amount of time required for clearing transfers remain high due to the intrinsic complexity of manually matching both counterparties' instructions that often involve multiple rounds of investigation. Similarly, corporate actions and dividends processing incur additional costs because they involve manual booking of notifications and corporate actions events. Total cost of transfers, corporate actions and dividends processing is estimated to be €120 million per year in Luxembourg.

- **Cash processing:** One payment per order and per counterparty remains the most common practice in the industry with few exceptions. This process has significant costs due to high volumes despite being highly automated. Currently, considering the cost of swift messages to issue and receive payments, the fund settlement processing in Luxembourg costs €170 million per year.
- **Compliance and record keeping:** To comply with Know Your Customer (KYC) regulations, the current industry practice consists in each management company collecting and verifying a set of documents (e.g., passport, ID card, utility bill) on each distributor. This model adds redundancy of requests received by distributors from all the fund promoters and results in processing overhead across the industry. The tasks involving KYC and due diligence cost €180 million to Luxembourg's industry annually.

4.2.3 Blockchain-based solution(s) and relevant initiatives

Blockchain has the potential to address several industry challenges ranging from significant reduction in the trade settlement time, increased transparency and traceability, costs mutualization, to name a few. Several initiatives in Luxembourg are exploring blockchain and distributed ledger technologies for the next generation funds management services and market infrastructure. Good examples of such initiatives are Fundchain [121] and FundsDLT [122].

Fundchain is a R&D initiative launched by a Luxembourgish start-up called Scorechain S.A. and is supported by various major industry players. This initiative has unveiled a Proof-of-Concept called SmartTA. FundsDLT is a result of collaboration between Fundsquare, InTech, and KPMG Luxembourg. It is a decentralized orders processing engine based on DLT, digital tokens, and smart contracts. Based on these works, the rest of this section describes how blockchain could transform existing funds distribution operational processes (and address the challenges discussed above). Section 4.2.4 then outlines the extent to which the costs incurred due to operational processes could be reduced.

Funds distribution platforms based on the blockchain technology could potentially offer greater (cost and temporal) efficiency to the value chain. For instance, orders processing and cash settlement could be encoded as smart contracts (and deployed on a blockchain) where the former routes the order from the investor to the TA/fund and the latter orchestrates cash movement. In contrast to the existing practice, the revamped operational model will allow investors to have direct access to available funds and perform subscription/redemption operations simply using an interface (e.g., mobile app, web portal) provided by the platform. In the simplest case, asset managers will sell their funds to the investors as follows [123]:

1. Investor sends a subscription order using an interface of the blockchain application.
2. The investor's subscription order triggers the orders management smart contract deployed on the blockchain (e.g., Order Management System – OMS – smart contract in FundsDLT).
3. The smart contract performs necessary checks on the investor and fund characteristics. If successful, the order is accepted and the settlement process triggered.
4. The NAV is computed by the fund accountant and sent to the blockchain network. After a series of validation checks, the transaction is settled and accounts updated.
5. The investor can view the entire process, track the status of the transaction at each step, until the final transaction confirmation.

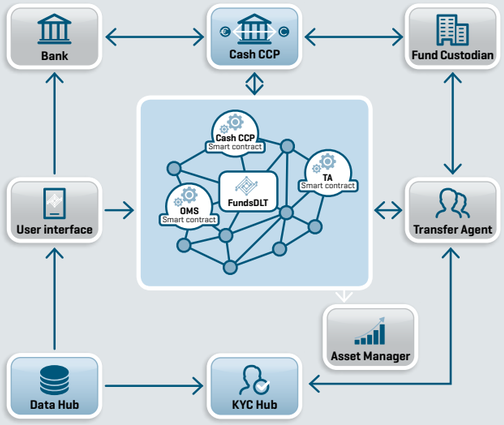
Similarly, the Anti-Money Laundering / Know Your Customer (AML/KYC) process performed to verify a client's identity could be transformed by introducing a KYC Hub to the blockchain network and the overall process could be as follows [123] [122]:

1. A new investor provides necessary identification details (e.g., passport, ID card, utility bill) to a trusted party called the KYC Hub.
2. After successfully completing the (initial) verification processes, the KYC Hub archives the investor's documents in a secure manner in the blockchain and provides a unique digital identity to the investor.
3. For any recurrent AML/ KYC procedures, the investor could simply provide digital identity and authorize management companies/distributors to perform necessary checks without going through the entire AML/ KYC process each time.
4. Management companies/distributors could query the trusted KYC Hub based on relevant regulations and verify the identification details of the investor.

Note that the same KYC Hub could be part of multiple blockchains and provide investors with the same services across different business networks. This could reduce the compliance costs and increase the reactivity to accept new business relationships.

These revamped operational processes not only eliminate redundancy and reduce the time to perform transactions but also improve flexibility (along with transparency and traceability) for investors and asset managers.

FundsDLT



FundsDLT network consists of the following components:

- FundsDLT is built as a private and permissioned blockchain that uses Ethereum (see Section 2.3) and provides consortium consensus.
- It incorporates three smart contracts that perform unique functions:
  - The **Order Management System (OMS) smart contract** performs order routing and creates the investor accounts. It routes the order from the investor to the TA and executes Delivery-Versus-Payment of shares against cash on the TA and investor accounts.
  - **Cash CCP (Central Counterparty Clearing) smart contract** converts fiat currency into coins/tokens (currently, not using cryptocurrencies but) according to a principal of tokenization. FundsDLT acts as an orchestrator for the cash movements when mirrored on the cash clearing account on the blockchain.
  - **TA smart contract** creates shares in the blockchain on the TA account and delivers them to the OMS smart contract.
- FundsDLT allows distributors and asset managers to plug digital orders interface to the network. Similarly, it integrates cash clearer solution with APIs that allow sending payment instructions and conducting cash settlements.
- A KYC solution is integrated to cover investor onboarding.
- FundsDLT will be able to accept and deliver transactions via SWIFT. In addition, an API based on the same standards as the one from PSD2 has been developed, and it allows to transfer transaction requests from an interface to the FundsDLT network.
- The Fundsquare data hub is incorporated within the FundsDLT design to allow for retrieval of fund information.

Using FundsDLT, the operating model sees an investor going through an application to access fund information and performing KYC duties, then processing an order by provisioning cash through a digitalized token. On the other side, transfer agents will perform the validation of KYC requirements and order acceptance, while an asset manager can follow-up on inflows and outflows in the registrar in real time. Once the Net Asset Value (NAV) has been published, the entire settlement process is executed instantaneously.

FundsDLT is expected to reduce the cost and processing time of transactions and investors, asset managers, custodian banks and transfer agents will be able to share information in a simpler manner. The ecosystem created by FundsDLT is designed to streamline AML/KYC and MiFiD verification by standardizing the process and streamlining repetitive tasks. FundsDLT intends to deliver an ecosystem by leveraging existing accounts, transactions, onboarding, KYC, payments and entitlement services. This is expected to lead to broader changes in Luxembourg's pool of expertise, enrich the current order management services, and enable Fundsquare [124] to provide more value-added services.

4.2.4 Economic impact and business opportunities for the funds distribution industry

As discussed above, blockchain-based solutions have the potential to streamline operational processes and increase efficiency in funds distribution. They would help create a decentralized yet unified ecosystem of activities related to asset managers, distributors, investors and service providers (see Table 21) [125].

Market player	Potential business opportunities
Asset managers	The revamped approach to orders processing could create the following opportunities. • Thanks to improved transparency, asset managers can develop better products that are aligned to the right client segment and meet the needs of unique client investors. Currently this is infeasible given the lack of direct contact between investors and asset managers. • Reduces the number of intermediaries in the investment process, which in turn will reduce the cost of fund distribution while providing better and controlled services to clients. • Asset managers could enhance client experience, improve marketing, and increase brand awareness.
Distributors and investors	Investors could optimize their fund selection strategy while distributors could ensure cost effectiveness and risk reduction. • Access to a range of available funds. • Reduce costs and risks of outsourcing order routing, settlement, corporate actions and sub custody to consortia of partners. • Increase revenues due to availability of better investor-focussed products.
Service providers	• Reduce intermediary costs while creating value added services and improve margins. • Create innovative services and products (e.g., better data analytics, robot advisors). • Enable easy access to international investors benefiting fund managers. • Improve trust through greater transparency in terms of fees and business transactions.

Table 21: Potential business opportunities for market players in funds distribution

Besides the revenue gains due to business opportunities (see Table 21) that blockchain based funds distribution ecosystems will create, cost savings could be achieved due to efficient mutualization of data sharing and orders processing through a central counterparty. The rest of this section discusses the latter aspect (cost savings) in detail.

As opposed to the current cash processing practices (see Section 4.2.2), consider the practice of netting per currency across counterparties and transaction types as an example. This practice would significantly reduce costs: in an ideal world, each market player would process one payment per value date and per currency, independently from the number of counterparties it deals with. Following the effect of volume compression, via the use of a central cash compensation account, the same activity would diminish costs (see Figure 23) [119].

In general, US achieves a higher degree of operational efficiency and cost mutualization than European counterparts. However, cross-border domiciles (i.e. Luxembourg) are more cost-efficient than other European domiciles (e.g., France, Germany and the UK) when it comes to multiple market distribution [8]. Given that there is limited potential for further cost reduction through cross border platforms, Luxembourg could further benefit by performing four key activities within the distribution supply chain [119]:

1. Tackle the residual portion of manual orders and reduce the cost of bilateral connections.
2. Increase automation beyond order management.
3. Cash netting with a central compensation account as a way to achieve high rates of payment compression.
4. Mutualize KYC and distributor due diligence procedures.

These activities could save up to 70% of total distribution costs for Luxembourg's industry (representing €900 million of annual savings). Figure 23 shows the estimated cost savings achieved by streamlining individual activities of the funds distribution supply chain [119]. Note that this streamlining could efficiently be achieved using platforms such as FundsDLT.

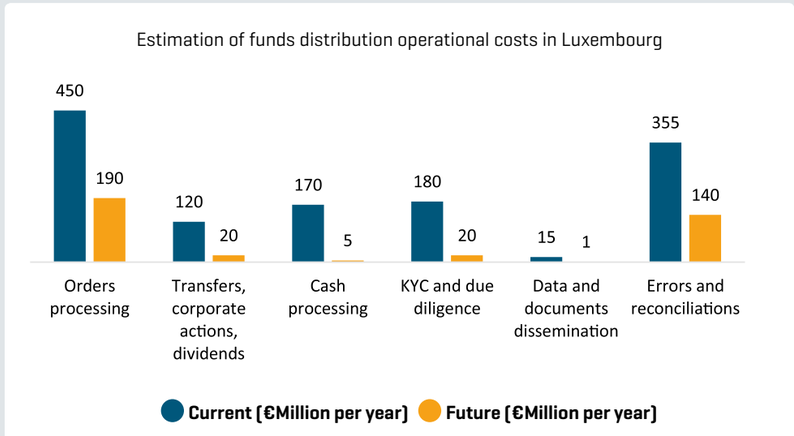


Figure 23: Estimate of annual operational costs in Luxembourg [119]

The impact of blockchain on funds distribution is beyond cost savings and has the potential to transform the overall sector. Note that full-fledged adoption of blockchain-based solutions for funds distribution might result in addition of operational processes. For example, a new market player or an existing entity might need to perform new activities such as:

- Membership management in the blockchain consortium.
- Administration and maintenance of smart contracts.
- Management of the overall technical infrastructure.

4.3 Case study 2 - Logistics and supply chain management

Logistics can be defined as the management of the flow of goods from the point of origin to the point of consumption. It usually comprises operational activities such as handling, transportation, packaging, inventory and warehousing. Supply chain management extends this definition of logistics with tactical planning and controlling in order to strengthen the relationships between the entities connecting the points of origin and consumption. It involves effective implementation of forward flow as well as reverse flow of resources such as goods, services, money and relevant information. As an example, Figure 24 illustrates a simple schema of a supply chain where the downstream material/goods flow is complemented by an upstream financial flow and various bidirectional information flows. Typically, the goal of logistics is to achieve the seven right of delivery: the right product, quantity, condition, place, time, customer, and cost [126].

4.3.1 Typical business model

Supply chain management essentially consists in managing three different flows: material flow, information flow and financial flow.

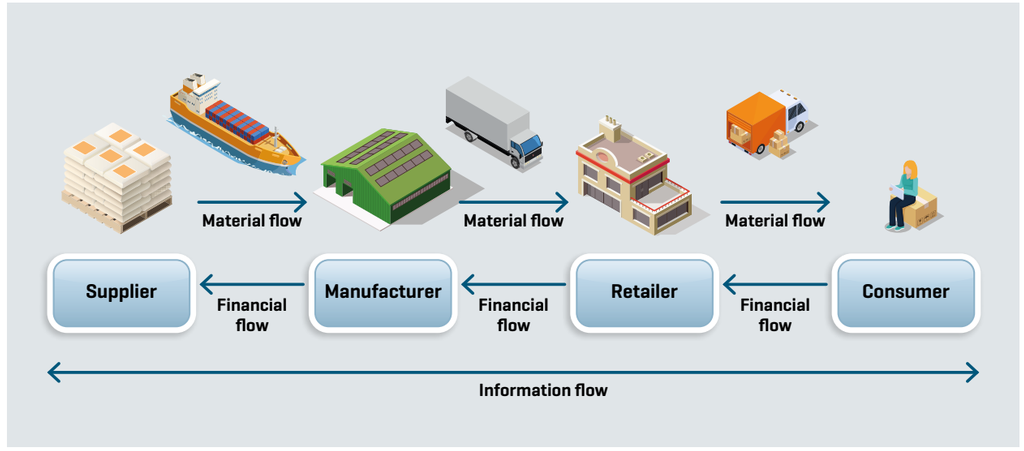


Figure 24: Simple schema of a supply chain with material, information and financial flows [126]

Material flow: In today's connected world, many players are intervening in the supply chain of a product. For the sake of generality, this case study considers abstract entities representing importers and exporters within a supply chain. For example, the supplier in Figure 24 is an exporter who produces and delivers raw materials to manufacturing companies (importers in this case) using logistics service providers. After production, a manufacturer in turn exports and sells products through retail companies (importers), and so on. This abstraction allows deeper analysis of various processes and flows between entities (importer and exporter) within a supply chain.

Information flow: Proper information exchange between an importer, exporter and logistics service provider builds trust and eases avenues of doing business. On the one hand, information flowing downstream to the next entity in the supply chain (e.g., status of a shipment) helps in improving planning and synchronization of future activities. On the other hand, upstream information (e.g. planned order volumes) helps in better fulfilling customers' needs. Well-managed information flows not only simplify tracking and tracing for importers and exporters but also eases the task of verifying the legitimacy and accounting of products for the administration (e.g., pharmaceuticals imported to the country).

Financial flow: As discussed above, the downstream material flow is often accompanied by an upstream financial flow. While end consumers generally pay immediately for the products purchased, the upstream supply chain partners (exporters) could experience a latency of multiple months. To mitigate trade risks, importers and exporters leverage trusted financial institutions (FIs) such as banks and insurance companies as intermediaries [103]. These FIs provide assurance to exporters (in situations where an importer does not pay) and contract certainty to importers (in the events where goods are not received). In addition to improving risk appetite of importers and exporters as well as monitoring counterparty performance, FIs document payment and delivery terms in letters of credit or open account contract vehicles. The importers and exporters pay fees to FIs for documentation and oversight of payment terms and for taking on the risk position. This financial flow/process is also referred to as trade finance [103]. The study published by the World Trade Organization [127] indicate that $18 trillion of annual trade transactions are estimated to involve some form of finance (credit, insurance or guarantee) globally. For the sake of completeness, this case study considers trade financing to be an integral part of supply chain management.

While blockchain could potentially play a role in all three flows, the aspect of trade financing within supply chains has been studied at a greater depth today (e.g., the World Economic Forum has studied trade finance as a use case in [103]). This aspect is also the main focus of this case study.

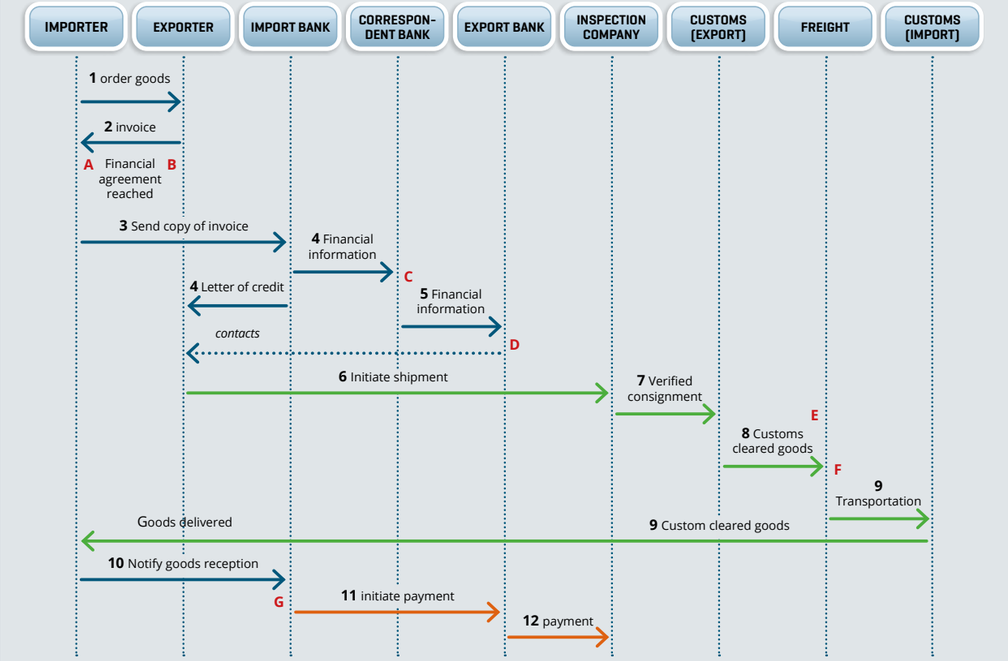


Figure 25: Representative trade finance model within supply chain management [103]. The numbers correspond to the steps in Table 22 and letters in the red font represent challenges (see Table 23). The green lines denote material flow, orange denote financial flow and all other steps denote information flow explicitly.

Figure 25 represents operational processes of trade finance between an importer and an exporter. Table 22 extends Figure 25 and describes each step in the process using three operational phases (establishment of agreements, goods delivery/logistics and settlement). Note that the model presented here focusses on a single import-export pair while similar operations are required across the supply chain, possibly with the involvement

of different logistics service providers, FIs and contractual terms, making the overall supply chain management a complex domain.

Establish agreements	Goods delivery	Settlement
1. Importer and exporter agree on the trade of a product. 2. An invoice then captures the financial agreement (point 1) by recording the quantity of goods, price and delivery timeline. 3. Importer provides a copy of the invoice to the bank for its review. 4. The `import bank' reviews the financial agreement and provides financials on behalf of the importer to a `correspondent bank' (which has established a relationship with the `export bank'). 5. The export bank provides the exporter with finance details, which enables the exporter to initiate the shipment.	6. When the exporter prepares the shipment, a trusted third party inspects the goods and verifies if the consignment is in line with the invoice. 7. Customs agents within the export country inspect the shipment and goods. 8. The goods are transported to the importer. 9. After customs clearance at the import country, the goods are delivered to the importer. Multiple modes of transportation (ship, aircraft, truck, train) and intermediary warehousing could be used in points 8 and 9.	10. The importer, upon receiving the goods, provides a receipt notice to the import bank 11. The import bank then initiates the payment to the export bank, via the correspondent bank.

Table 22: Operational processes of trade finance within supply chain management [103]

4.3.2 Industry challenges

If it is agreed that digital transformation will help in increasing the efficiency of logistics and supply chain management, its implementation is currently lower and lacking behind, as compared to other economic sectors [126]. For example, when shipping a container of perishable goods from East Asia to Europe involves nearly 30 different organizations and they exchange information on approximately 200 different events, often through printed paperwork [126]. Such paper-based processes result in inefficient, error-prone, time-consuming and fraud-sensitive supply chains. For instance, estimates indicate that 10% of all freight invoices have inaccurate data, which leads to disputes and inefficiencies in operational processes [128].

Another source of challenges in today's supply chains are due to numerous intervalence and interactions from manufacturing to final delivery of the product. This, in addition to the large number of stakeholders involved in supply chains, often create low transparency, unstandardized processes and data silos.

This situation may result in the following pain-points to the industry:

- **Traceability:** The prevalent information management methods across supply chains induce operational risks and lack tools to control damages. For instance, due to poor information traceability along the supply chain, sometimes it is challenging to know whether the products (e.g., perishables) have been stored/transported under the right conditions, inducing operational risks. Similarly, since information providing sources (factory or warehouse from which each pallet or container originated) of the inventory could not always be determined instantaneously, it is difficult to control potential damages. Note that the current system of documenting information is unable to meet the growing demand among consumers in knowing detailed information about the products they use (e.g., origin of materials and entities involved in the supply chain) be it food, apparel or electronics.

- **Inefficiencies:** Similar to the information flow, financial flow largely remains a paper-based business. For example, the bill of lading[52] received when a trader ships goods is paper-based, which should then be sent by courier to the bank for obtaining a letter of credit, making the overall process relatively slow (as compared to a digitalized process). In fact, the costs of administration and paperwork processing are estimated to surpass 15% of the actual transportation costs [129].
- **Cases of fraud:** The inefficiencies in the current system have resulted in regular cases of fraud with the bills of lading, posing losses for banks as well as traders.
- **Transparency and coherence: T**he need to provide up-to-date information across entities within a supply chain remains an open challenge. This lack of streamlined information flow is one of the root causes for the abovementioned challenges and the problem is exacerbated because of the lack of data standards, leading to a situation where each entity operates on different platforms/formats.
- **Compliance costs:** Banks and corporates must perform thorough checks on their customers (due diligence and KYC) to verify that a transaction does not result in money laundering, terrorist financing or export of restricted goods. The survey [130] indicate that 30 percent of 722 corporate respondents have spent more than two months for on-boarding new clients while 10 percent of them claim to have spent four months.

In contrast to the major pain-points discussed above, for the sake of better understanding, Table 23 lists challenges categorized as the same operational phases (establishment of agreements, goods delivery/logistics and settlement) as Table 22, based on [103] and [131]. The letters in Figure 25 also indicate these challenges at different steps of the supply chain model.

Establish payment terms	Goods delivery	Settlement
A. **Manual contract creation:** the import bank reviews the financial agreement manually and sends financials to the correspondent bank. B. **Invoice factoring:** exporters use invoices to achieve short-term financing from multiple banks, adding additional risk in the event the delivery of goods fails. C. **Manual AML review:** the export bank manually conducts KYC/AML checks on the financials received from the import bank.	D. **Duplicative bills of lading:** the inability of banks to verify the authenticity of the bills of lading result in their use (fraudulently) multiple times for gaining credit. Similarly, duplicate or inaccurate bills are also an issue for other stakeholders in the supply chain. E. **Delayed timeline:** intermediaries and numerous communication points delay the shipment of goods due to multiple checks, which are paper-based. F. **Lack of visibility:** information about the storage and transportation conditions of products along the supply chain is often unavailable.	G. **Multiple versions of the truth:** significant version control challenges exist to maintain financial information of each transaction. H. **Delayed payment:** before disbursing funds to the export bank, multiple intermediary processes verify that goods are delivered to the importer as agreed a prior.

Table 23: Challenges in trade finance within supply chain management [103] [131]

[52] A detailed list of cargo in the form of a receipt given by the transport company to the organization consigning the goods.

4.3.3 Blockchain-based solution(s) and relevant initiatives

Blockchain provides a new way to record provenance across complex supply chains, to automate enforcement of agreements by means of smart contracts, and to address various other existing challenges. The use of blockchain in supply chains has attracted significant attention globally from giant retailers to shipping ports and from steel to valuable commodities such as diamonds and artwork. Some examples of such initiatives are listed here:

- Walmart, IBM, Chinese retailer JD.com and Tsinghua University have formed a Blockchain Food Safety Alliance to improve food traceability and safety. Pilot testing indicates that by applying blockchain to trace a package of mangoes from the farm to the store took about two seconds (as compared to days or weeks earlier)[53].
- The Danish shipping company Maersk has completed a proof-of-concept trail for marine insurance with Microsoft, Willis Tower Watson and other insurance companies[54].
- Maersk and IBM are developing a global trade platform using the blockchain technology to improve the cost of transportation, lack of visibility and inefficiencies in existing supply chain (paper-based) processes[55].
- The Port of Rotterdam established BlockLab to study blockchain for energy as well as logistics[56]. This project claims that blockchain has helped in increasing compliance and transparency, better tracking of assets and orders, as well as resolving trust issues in port logistics [132].
- 16 companies in The Netherlands, led by TKI Dinalog – a Dutch Institute for Advanced Logistics – is exploring how DLT can boost efficiency and effectiveness, and reduce supply chain footprints[57].
- Deloitte Luxembourg has developed a proof-of-concept ArtTracktive to track movements of art works.

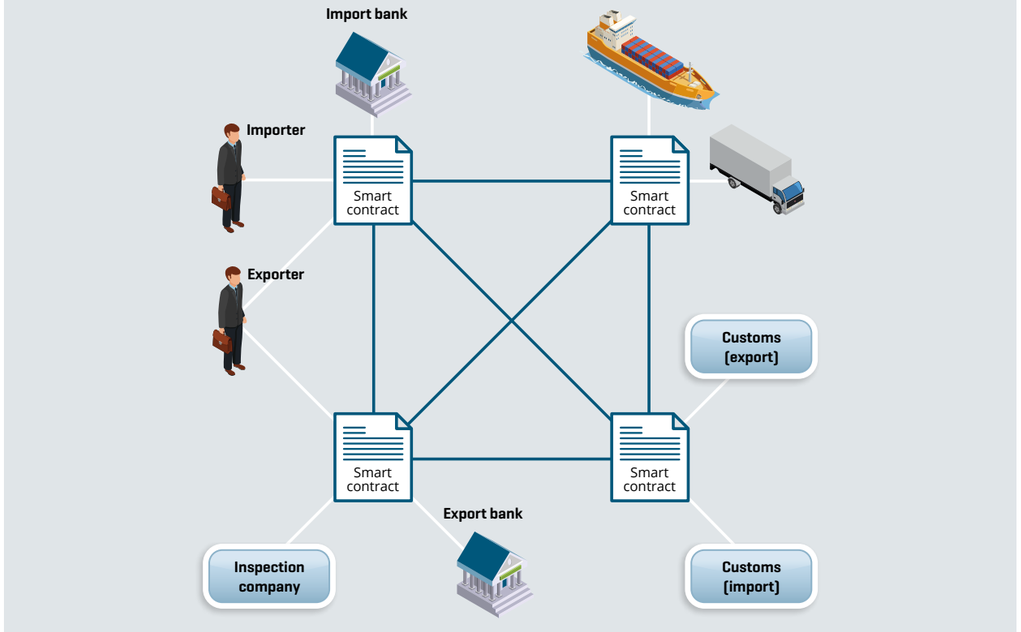


Figure 26: Revamped supply chain business model

[53] https://www.forbes.com/sites/rogeraitken/2017/12/14/ibm-walmart-launching-blockchain-food-safety-alliance-in-china-with-fortune-500s-jd-com/#5f2cfe337d9c

[54] http://fortune.com/2017/09/05/maersk-blockchain-insurance/

[55] https://www.coindesk.com/shipping-blockchain-maersk-spin-off-aims-commercialize-trade-platform/

[56] http://www.blocklab.nl/

[57] https://www.dinalog.nl/

Figure 26 illustrates how blockchain and smart contracts could revamp the typical business model (supply chain) described in Section 4.3.1. Table 24 then describes the steps in the revamped trade finance process within the supply chain model using the same operational phases as in Table 22 and Table 23. Transactions at each step are securely recorded in the blockchain.

Establish payment terms	Goods delivery	Settlement
1. An importer and an exporter agree on the trade of a product. 2. Using a smart contract, an invoice capturing the financial agreement is generated and shared with the import bank. 3. The import bank (facilitated by smart contract) reviews the agreement, drafts the letter of credit, and sends it to the export bank for approval. 4. The export bank reviews the letter of credit and generates a smart contract encoding terms and conditions of the letter of credit.	5. Exporter digitally signs the letter of credit and initiates the shipment. The bill of lading (which is the contract between the exporter and the carrier) would then also be on the blockchain. 6. The inspection company verifies the consignment and the customs agent within the export country checks the shipment (both entities potentially as nodes in the blockchain network). The clearance from these parties is received by means of a digital signature. 7. The goods are transported and delivered to the importer after customs clearance at the import country similarly to step 6. 8. If applicable, information on the storage/transportation conditions are recorded on the blockchain along the supply chain.	9. The importer digitally acknowledges the receipt of the goods, which triggers the smart contract and the payment from the import bank to the export bank is carried out.

Table 24: Operational trade finance processes in a transformed (blockchain-enabled) supply chain model [103]

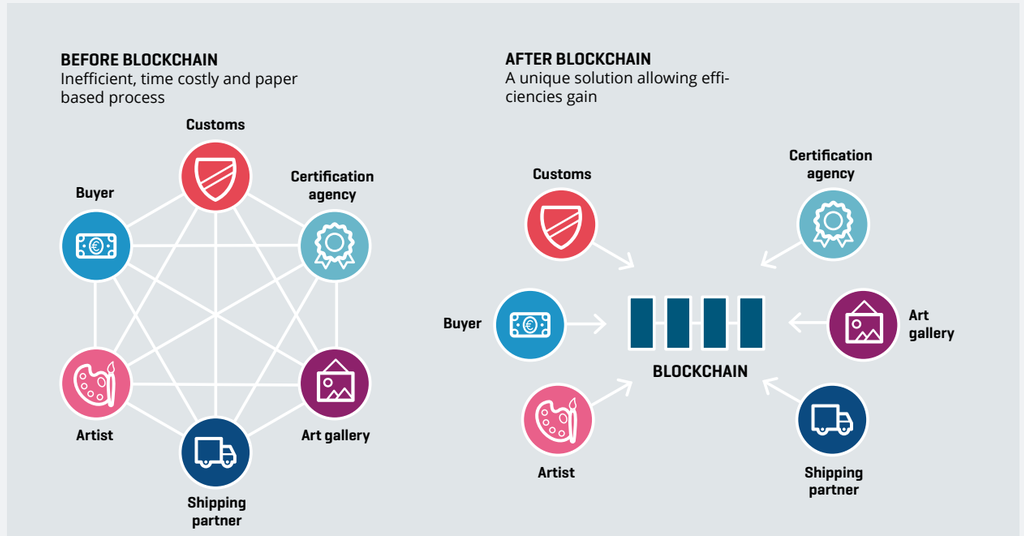
Moving beyond, the fusion of blockchain and IoT could create a number of opportunities for the logistics industry in general and more so for track-and-trace applications. For instance, consider that physical products are tied to IoT sensors that record and autonomously transmit data about the product's condition (e.g., temperature, location). This data could be used to ensure product integrity and as evidence against product tampering. Similarly, data about how goods are made, where they come from, and how they are managed could be collected with the help of IoT devices and stored on the blockchain. This information could then be used by companies to automatically provide proof of legitimacy (e.g., for pharmaceutical shipments) and authenticity (e.g., for luxury goods).

ArtTracktive

According to the TEFAF 2016 Art Market Report, in 2016, $63.8 billion-worth of art was sold globally and the number of art transactions in the world reached 38.1 million.

Due to the paper-based nature of art transactions, there are numerous provenance and traceability issues related to artworks. The players of the art market still rely on paper certificates and receipts which can easily be lost, tampered with or stolen – and history has shown that fraudulent certificates of authenticity are not uncommon.

As a response to these challenges, Deloitte Luxembourg has developed a technological alternative to the paper trail and fragile documentation that normally prove the provenance and track movements of arts.



Deloitte Luxembourg's ArtTracktive proof-of-concept demonstrates how blockchain technology can solve the current provenance and traceability issues by tokenizing an art work and storing on a distributed ledger its full transactional history in a secure environment available to all.

This software application manages and traces the interactions between all parties involved, from the artist or the owner, via freight forwarders, customs, art galleries, museums and all the way to potential buyers or lenders. Deloitte is currently in discussion with technology providers to secure a strong link between the token, i.e. the digital equivalent of a physical object, and the art work itself.

4.3.4 Economic impact and business opportunities for the supply chain and logistics sector

Logistics is an international trade oriented business and is a vital component of today's globalized world. In the year 2015, Luxembourg had an estimated 750 companies related to logistics with an overall turnover of €4.4 billion and the gross income (value added factor costs) of €1.15 billion [133]. The number of persons employed by this sector during the same period was over 12,500, underscoring its major contribution to the country's economy. This implies that achieving new efficiencies in logistics could have a direct and significant impact on the economy.

As discussed above, blockchain-based solutions have the potential to transform existing processes and increase efficiency in supply chains. They would help create a decentralized yet unified ecosystem of activities related to various entities (importer, exporter, banks, customs) and flows (information, finance and material) in the supply chain, thus achieving cost savings with leaner, more streamlined and automated error-free processes. The World Economic Forum estimates that reducing supply chain barriers to trade could increase global GDP by nearly 5% and trade by 15% [134]. Maersk and IBM expect their blockchain-based solution designed to track millions of shipping containers to not only reduce delays and fraud but also lead to billions of dollars in savings to the industry.

Finally, the visibility and predictability of logistics operations could be increased, the flow of goods could be achieved in significantly lower time, and sustainable supply chains could be enabled with provenance tracking and by tackling product counterfeiting. These benefits could transform the industry with new logistics services and more innovative business models. For the sake of completeness, Table 25 highlights some benefits of blockchain-based solutions following the three categories used in the rest of this case study.

Establish payment terms	Goods delivery	Settlement
Speed and scalability: Documents relating to financial agreements (e.g., invoices) will be accessible to relevant entities via a distributed ledger thus making the review and approval process easier. Consequently, the amount of time needed to initiate the shipment would also reduce. **Transparency:** The near-real time access to up-to-date information could help in better planning of future activities. For instance, access to invoices could improve short-term finance planning for importers, exporters as well as banks. **Disintermediation:** blockchain could potentially allow 'import bank` and 'export bank` to finance importers/exporters and assume risks without collaborating with the correspondent bank (trusted third party).	**Reduce frauds:** The potential for double spending could be eliminated by tracking bills of lading. Similarly, since different administrations need to perform different checks for certain products and validate those checks on the blockchain, the flow of cargo through those checks is eased up. **Traceability and visibility:** chronological recording of each transaction provides a tamper-resistant trail of activity throughout the business process. The right transportation and/or warehousing conditions that need to be respected (e.g., for temperature-sensitive products), could be traced along the supply chain, reducing operational risks and providing tools to control damages. **Provenance:** blockchain serves as the data registry where the proof of ownership is automated and trustworthy. **Decentralization:** when contract terms are satisfied, the system automatically executes relevant activities (e.g., notifying the import banker) in near-real time, significantly reducing the time and costs of administering the delivery of goods.	**Automated settlement and reduced operational costs:** smart contracts trigger settlement terms when relevant conditions are met, thus eliminating the need for correspondent banks as well as reducing transaction fees. **Reduced costs of regulatory compliance (e.g., KYC).**

Table 25: Potential business opportunities with blockchain-enabled trade finance within supply chains [103]

4.4 Case study 3 – Digital identity and data exchange

Identity is a collection of attributes that describe a user. These attributes comprise a set of personal or sensitive data claimed by the user and verified by a trusted party. Given that a wide variety of the set of attributes exist, the World Economic Forum [135] has broadly classified attributes into three groups: inherent (e.g., biometric fingerprints, date of birth), inherited (e.g., citizenship) and assigned (e.g., phone number) attributes. These attributes intrinsically differ for different types of user groups such as natural persons, enterprises, devices and processes.

A digital identity is a set of digital records that represents a user. In an increasingly borderless and digital world, digital identities are becoming a norm and digital identity systems allow personal or sensitive data delivery along with its supporting documentation and validations to service providers. Service providers require a digital identity system to accept or deny transactions as well as to customize and provide better user experience.

4.4.1 Typical business model

Identity is foundational to many systems and services – it enables users to participate in transactions, by proving to their counterparty (such as a service provider) that they have the specific validated attributes required for that transaction and thereby create a degree of trust. From a service provider's point of view, a user must satisfy at least three main aspects of identity [135]:

- **Attributes:** The user must present the proof of attributes, which is in turn validated by the service provider.
- **Authentication:** The service provider must determine whether the attributes match the presenting user. A given transaction is allowed only if the user has been authenticated.
- **Authorization:** Based on the type of transaction, service provider must establish the requirements for transaction eligibility and query relevant attributes (e.g., date of birth, address) from the user.

Note that service providers conduct these activities to different degrees of sophistication based on the risk/value of each transaction and considering the acceptable level of assurance.

To put into context, consider a typical customer's journey while purchasing an insurance policy for an apartment today:

1. User clicks to subscribe and enters the personal data requested to receive credentials used for authentication.
2. User authenticates her email in order to establish a first degree of trust. User also authenticates to the system and provides necessary personal data about her apartment such as address, apartment size, value and condition *(attributes)*[58].
3. Insurance company customizes an offer and sends to the user a proposal and contract conditions via an email or post.
4. User provides her identity document and proof of residence document over email or post *(proofs and supporting documentation)*. Insurance company validates the attributes and their supporting proofs. After initial validation (authentication), the insurance company generates an application form and sends a contract for the user to sign by post.
5. User reviews and fills in the application form and contract with lacking data; she signs and sends the application form and the contract to the insurance company by post.
6. Finally, user receives the SEPA contract via post. She must fill in the bank details, sign the contract, and send the agreement via post.
7. The same procedure needs to be repeated if she made a mistake, wants to change some attributes or wants to change the insurance company.

[58] The aspects of identity are provided here as examples – to facilitate a better understanding

4.4.2 Industry challenges

The challenges in the existing identity management systems are wide ranging and are discussed here in three categories: challenges to the system itself (e.g., need for better trust models, streamlined service delivery, lack of transparency), challenges related to data management (e.g., security and privacy, increasing transactions volume), and challenges related to regulations.

Identity management systems: The purpose of an identity system is to allow counterparties with no previous relationship to establish trust in executing a transaction. However, today's transactions increasingly involve very disparate entities (e.g., customers and businesses transacting cross-border), where different trusted third parties attest an individual's attributes, using different methods of authentication. Moreover, customers are increasingly expecting seamless, omni-channel service delivery, and tend to migrate to other services that offer better customer experience. Customers also expect that their identity would be re-usable in any kind of service providers' environments.

Another set of user demands consists of providing increased visibility into which attributes would be exposed and to what entities during digital transactions. However, current approaches do not allow companies to assess the accuracy of validations or to trace the process, resulting in a lack of transparency. Recently, the citizens of Estonia for example were given the ability to view who accessed their records, how often and for what purpose [110]. This transparency allows citizens to feel ownership over their data, as they are able to see how information related to them is being used.

Data management: The current centralized systems require service providers to store and manage Personally Identifiable Information (PII) of their customers for extended periods of time, thus placing significant trust in them, and leaving them liable for handling PII. The challenges arising from this aspect exacerbates due to the following issues:

- Centralized solutions have evolved to address the growing business needs for remote, digitized services and the benefits of having a large data set regarding customers. However, they are prone to data breaches and present a single point of failure. The impact of data breaches and failures becomes widespread with poor business practices concerning data handling and manipulation.
- The number of identity-dependent transactions is growing through increased use of digital channels and increasing connectivity between entities.
- The design of the centralized system needs to be as generic as possible, while defining exactly the needs of service providers (e.g., the format in which attributes are to be received and the contexts in which they are applicable). Failure in carefully defining these needs result in various challenges of interoperability. For instance, address formats, insurance numbers and so on, differ depending on contexts.

Nevertheless, for many users, data management centralized and managed by a renowned trusted third party, may feel safer than data-distributed alternatives.

Regulations: Regulators are demanding increased transparency around transactions and are holding service providers liable for inaccurate or missing identity information. For instance, financial institutions face growing compliance challenges related to identity, with Know Your Customer (KYC) costs that can reach up to $500 million per year for large banks. As a result, financial institutions require greater granularity and accuracy in the identity information they capture.

On the other hand, strict data privacy rules such as the European General Data Protection Regulation (GDPR) limit the ability to access validated customer identity attributes with potential fines up to €20 million or 4% of annual revenues [135]. Adversaries are gaining access to sophisticated technology and tools that could quickly cause financial and reputational damage by exploiting weak identity systems.

4.4.3 Blockchain-based solution(s) and relevant initiatives

Blockchain could be used in identity applications as an information storage and transfer mechanism within numerous use cases. For instance, users could store their identity attestations on a ledger and share them with different service providers using the underlying distributed protocol. Similarly, in a private and permissioned blockchain where the ledger would be owned by a single entity, a consolidated view of the users' attestations would be provided for use in transactions, while concealing the information about the nature of the credentials. Table 26 lists various properties that an identity system (and by extension private data management system) requires and compares these properties with public blockchain, permissioned blockchain and permissioned-centralized system.

	Permissionless Public blockchain	Permissioned blockchain	Permissioned Centralized system
Regulatory compliance (e.g., GDPR, PSD2, eIDAS)	No	Yes	Yes
Data availability (SLA)[59]	No?	No?	Yes
Erasure and rectification	No	No	Yes
Performance and scalability	No	Yes?	Yes
Data interoperability	?	Yes?	Yes
Privacy by design	No	Yes	Yes
Immutability	Yes	Yes	Yes
Full end-user control	Yes?	Yes?	Yes?
Transparency and auditability	Yes	Yes	Yes
Transaction maintenance	Yes	Yes	Yes
User experience	Yes?	Yes?	Yes

Table 26: Applicability of attributes of an identity system in a centralized system, public blockchain and permissioned blockchain

A blockchain-based identity management system could be viewed as a tool for cutting the paper process during verification of identity documents and a form of decentralized signature sharing to provide truly decentralized attestations. For the sake of better understanding, consider again the example of buying an apartment insurance. This system would involve the following steps in executing a transaction:

1. The first time/new user must undergo an initial registration process (similar to the one described in Section 4.4.1), install relevant app and provide consent to manage her personal data. Thereafter:
2. User clicks to subscribe and logs in to the blockchain-based identity and data management platform.
3. User gives consent to sharing the existing attributes and proofs.
4. If necessary, user enters the new requested attributes as well as supporting documentation and gives consent to sharing them.
5. After providing consent, the user waits for a contract to be generated by the insurance company.
6. When ready, user signs the contract and the SEPA agreement electronically.

Several projects have been initiated and companies formed globally to realize a decentralized identity management scheme. In Luxembourg, LuxTrust S.A. is the biggest identity provider and EU-certified Qualified Trust Services

[59] In practice, identity information consists of a variety of strings, images, audio and pdf documents, which makes storage on a blockchain inefficient. Moreover, GDPR enforces the right of erasure that is incompatible with the blockchain technology in general. In this context, the availability of identity information is questionable (particularly on public blockchain) since it is extremely expensive.

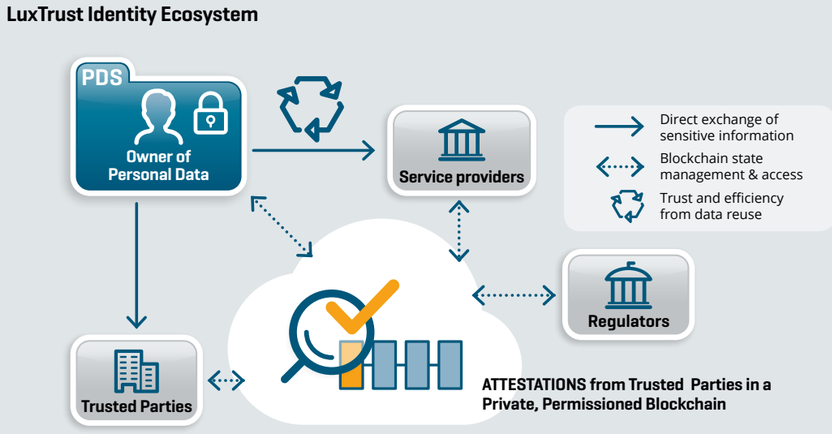
Provider, focused on certificate issuance and management, digital identification and electronic signature. LuxTrust S.A. and Cambridge Blockchain LLC, the Massachusetts-based digital identity enterprise software, are collaborating to develop a new privacy-protecting European identity platform (called LTID)[60].

LTID will offer businesses and consumers a trusted environment to exchange and manage personal data online, in compliance with GDPR. Applications will cover rapid onboarding and validation checks for financial service providers and other digital onboarding and digital KYC solutions in any sector, as well as a broad range of personal data sources such as health records and Internet of Things devices. In other words, LITD is an open ecosystem that connects customers, service providers and validators to enable them to collect, validate, exchange, audit and re-use personal data in a secure and GDPR compliant environment.

LuxTrust Personal Data Management & Exchange Platform (LTID)

LTID Platform revolves around 3 main types of users:

1. **Customer:** A customer seeks to obtain products and services from a provider, for which she may need to share identity and personal data verified by a trusted third party. For example, a customer can be an individual seeking a loan.
2. **Service Provider:** A service provider provides products and services to customers. The provider may seek identity and personal data – verified independently by a trusted third party – from the customer to offer the products and services. For example, a service provider can be a bank that sells consumer loans.
3. **Trusted Party (or Validator):** A trusted party verifies and attests a customer's data according to validation models it defined. An example of a trusted party could be a country's tax authority that attests an individual's previous year's annual income based on a filed tax return.



ROLE	ACTIONS	ACTORS
Owner	Owns and controls personal data	Natural persons, Enterprises, Devices
Trusted Party	Trusted verification (attestation) of data	Enterprises
Service Provider	Consumes personal data and attestations	Enterprises
Regulator	Oversees compliance	Supervisors

[60] https://www.cambridge-blockchain.com/single-post/2016/08/09/Event-1

All types of entities including end-users, corporate and institutional organizations can act as customers, service providers or trusted parties. In this way, all types of different use cases can be enabled. For example, a natural person (customer) might want to share some data with a company (service provider) with some validations done by a governmental organization (trusted party) in case of an insurance service. Similarly, a company (customer) might want to share some data with a supervisory body (service provider) with some validations done by an independent auditor (trusted party) in order to achieve certification or compliance with a specific regulation.

The LTID Service should be understood as enabling the sharing of data between at least two parties, a customer and a service provider, for a specified period of time under certain policies and user's consent explicitly given to the service provider. The LTID Service is meant to establish a legal contract between two parties that enables the sharing of sensitive data with trust, confidence and compliance. Such a contract allows the specification of what data is shared, for what purpose, the period for which it will be processed and allow the negotiation of additional policies. The parties involved are always strongly identified by LuxTrust eIDAS trust services and equipped with electronic certificate and strong authentication as well as legally binding signature service. LTID platform allows the tracking by, and provides reporting to, all parties involved in a transparent and immutable manner powered by blockchain technology so that clear records can be presented at any time on what data was shared, for what purpose, under what rules and for how long (thus matching GDPR reporting obligations).

4.4.4 Economic impact and business opportunities for digital identity

Currently, the identity in itself is not monetized; that is, the business model today consists of providing identity more-or-less freely and profits are made from underlying services and business transactions. In the near future, identity would become a service in itself. LuxTrust S.A. – as an EU qualified trusted service provider – is in an ideal position to provide a personal data management solution using business models [136] that directly monetize Personal Data [137].

Identity systems based on the blockchain technology will have the potential to competing challenges of transparency, privacy and better data protection, faster customer onboarding, lower costs, customized user experience and enhanced compliance through a single, trusted and consistent view of customer reference data. The need for intermediaries would reduce and efficiency, quality and re-usability of personal data and electronic identities would increase. Table 27 lists (although not exhaustive) opportunities to each party involved in the identity management system, based on [135] [137].

Market players	Potential business and economic opportunities
Users	• **Privacy and control:** users have greater control over their attributes and could define who has access to their data. • **Security:** user data and attributes are stored in a safe and secure manner (e.g., using blockchain properties such as tamper-resistance, immutability etc.). • **Convenience:** ability to perform transactions across various services in a cost-effective and efficient manner. • **Transparency:** users have near-complete visibility into how and when their attributes are used.
Identity providers and trusted parties (IdPs)	• **Revenue growth**: IdPs could build new business models and charge fees for processing identity transactions. • **Decreased risk and liability:** the consequences of data loss or breach are significantly clearer to IdPs; thus, they could develop better risk management approaches. • **Competitive positioning:** IdPs would become an integral part of the digital economy and will share strong relationship with users across sectors. • **Improved products and services:** IdPs could provide highly customized, detailed and trustworthy services.
Service providers (SPs)	• **Information accuracy:** SPs have access to trusted, verified identity information. • **Decreased transaction abandonment:** A streamlined user experience removes barriers to completing transactions. • **Service provision:** SPs will be able to differentiate between illicit and legitimate users with greater efficacy. • **Service tailoring:** Similar to IdPs, service providers could provide improved products and services and reduce risks and liability.
Regulators	• **Tracing of assets:** Regulators could trace asset origination and ownership effectively. • **Transparent view of entities:** Regulators can access an aggregated view of legal entities across their hierarchies. • **Improved compliance:** Regulators will be able to access trusted, up-to-date attribute information about users, and improve the effectiveness of the overall compliance process. • **Data standardization:** Data collection and storage could become a standardized approach across various institutions, reducing friction in data aggregation.

Table 27: Opportunities for different players in an identity ecosystem [135] [137]

5

Blockchain and DLT standardization

5. Blockchain and DLT standardization

The rapid technological advancements in blockchain and DLT as well as their adoption across economic sectors have warranted a careful study and growth of technical standards. For instance, use of standard architectures could enable qualitative development of decentralized applications and shared ledgers, and use of standard terminology could support effective communication and growth. As seen in Chapter 4, data standards are a prerequisite to streamline supply chains while standards facilitating interoperability are of at most importance to any use case where business partners need to collaborate for generating value. Similarly, availability of security and privacy standards are necessary for easy implementation of decentralized funds distribution and identity management platforms.

Standardization bodies at international as well as European levels have initiated activities that could increase market confidence in blockchain and DLT. This chapter provides an overview of various developments in the areas of technical standardization. After providing some background details about standardization (Section 5.1), this chapter first focuses on ISO/TC 307 given that this technical committee is prominent in standardizing blockchain and DLT (Section 5.2). The chapter then summarizes other initiatives launched by ITU-T (Section 5.3) and CEN/CENELEC (Section 5.4), and finally about developments with respect to digital trust (Section 5.5) and Smart ICT (Section 5.6).

5.1 Background on technical standardization and the national context

Technical standardization is a long-standing tool that is widely recognized for its ability to provide technical or qualitative referential for products, services or processes. Technical standards are developed by organizations that bring all interested stakeholders together and are active at different geographical levels in their own area of competence, as illustrated in Figure 27:

- At the **international level**, the three recognized standardization organizations are the:
  - International Organization for Standardization (ISO)
  - International Electrotechnical Commission (IEC) and
  - International Telecommunication Union's Telecommunication Standardization Sector (ITU-T).
- In the **EU**, the three recognized European Standardization Organizations [138] are the:
  - European Committee for Standardization (CEN)
  - European Committee for Electrotechnical Standardization (CENELEC) and
  - European Telecommunications Standards Institute (ETSI).
- Finally, **at national level**, each country has one national standards body (NSB) that protect the interests of the country within the European and international standardization organizations. In **Luxembourg**, **ILNAS** is the NSB and is member of the European and international standardization organizations: CEN, CENELEC, ETSI, ISO, IEC and ITU-T.

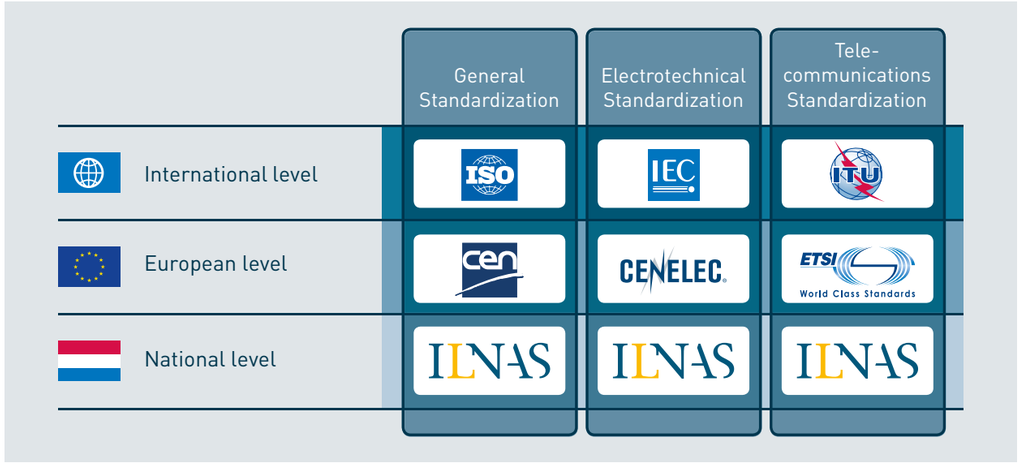


Figure 27: Standardization organizations and their scope of influence [139]

Technical standards provide an effective economic tool for achieving various objectives, such as mutual understanding, satisfaction, reducing costs, eliminating waste and improving efficiency, compatibility, security, performance, quality and reliability, convenience of use, trade, economic performance, accessing the latest knowledge and technology, providing positive perception and reputation of business. The application of the fundamental principles stated by the World Trade Organization, namely transparency, openness, impartiality and consensus, effectiveness and relevance, coherence and development dimension, throughout the development of technical standards, also guarantees the legitimacy of these documents.

Technical standards also play an important role for innovation. As pointed out by the European Commission (EC) in its communication Europe 2020 Flagship Initiative [140], standards enable the dissemination of knowledge, the interoperability between new products and services, and service as a platform for further **innovation**. This is all the more important in a world that tends to become digitalized and in which everything becomes connected. Technical standardization is thus a keystone to ensure the interoperability of complex ICT systems and it will contribute to erase the barriers that may still exist to build the future of the digital world.

ILNAS – with the support of ANEC GIE – works actively on the development of ICT technical standardization including in the blockchain and DLT areas. The Luxembourg Standardization Strategy 2014-2020 [141], approved by the Minister of the Economy, underscores the ICT sector as one of the cornerstones. Accordingly, Luxembourg's policy on ICT technical standardization 2015-2020 [142] provides guidance towards a number of activities to strengthen the national ICT sector's involvement in standardization work. It includes, beyond the management of several NMC and the creation of **education**[61] **and research**[62] **programs** in the standardization area, the development of reports to inform the market about current standardization developments in the ICT sector.

Main example is the annual publication of the Smart **ICT Standards Analysis** [143], which provides an overview of latest standardization developments of selected Smart ICT technologies (Cloud Computing, Internet of Things and Big Data), as well as the related Digital Trust standards-based evolution. This report also introduces, since 2018, current trends in Smart ICT, namely artificial intelligence and blockchain and DLT, and standardization developments in these areas. One of the purposes of this report is to serve as a practical tool to national stakeholders to identify relevant standardization technical committees in Smart ICT, and to offer them guidance for a potential future involvement in the standards development process [139].

[61] https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/projets-phares-dans-l_education-a-la-normalisation.html

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

5.2 ISO/TC 307 Blockchain and distributed ledger technologies

On April 14, 2016 – Standards Australia proposed to create a new ISO Technical Committee (TC) that would develop international standards in the areas of blockchain and DLT [144]. After a successful ballot among member states, the ISO Technical Management Board officially accepted the proposal during its 67th meeting on September 10, 2016 and Australia was given the responsibility of serving as the Secretariat of the newly created technical committee ISO/TC 307.

First plenary meeting – April 2017: The first ISO/TC 307 plenary meeting was held in Sydney, Australia from April 3—5 2017. The objectives of this meeting were threefold:

- To agree on the title and scope of the technical committee;
- To review and discuss the contributions provided by international experts participating in the TC in order to define its structure and future projects; and
- To establish liaisons with other TCs and external organizations in order to ensure collaboration with all interested parties.

The major outcomes of this meeting could be summarized as follows:

- The title of ISO/TC 307 was defined as "Blockchain and distributed ledger technologies" and its scope as "Standardization of blockchain technologies and distributed ledger technologies".
- Based on the contributions received from international experts, the technical committee decided to create five Study Groups (SGs)[63] [145] and one Working Group (WG)[64], as detailed in Figure 30. SGs were given the responsibility of analyzing the state-of-the-art in their respective domains and of providing a report with their recommendations to the TC before the next scheduled plenary meeting in November 2017.
- The Committee initiated its first project of drafting an International Standard that would define the terminology and concepts (see Table 28), under the responsibility of the newly formed WG, called "WG 1 Terminology".

Second plenary meeting – November 2017: The second ISO/TC 307 plenary meeting was held in Tokyo, Japan from November 14—17, 2017. The reports (and recommendations) developed by the SGs and WG 1 were discussed during this meeting. As a result, the Committee decided to adapt the structure of the TC by creating two new WGs (merging the work then carried out by SGs) and two new SGs (see Figure 30) [146]. These SGs and WGs were assigned several new projects that are detailed in Section 5.2.4.

Before providing details on these projects, this section outlines other aspects of ISO/TC 307 such as the current state of membership, liaisons, and the structure of the TC.

5.2.1 Members of ISO/TC 307

Figure 28 is a map illustrating the type and expanse of membership in ISO/TC 307. As mentioned above, Australia serves as the Secretariat and Chair of the TC. It currently has 30 Participating Members (P-members), including Luxembourg, and 12 Observing Members (O-members). For a newly created TC, these memberships demonstrate a great interest in the TC's activities from around the globe.

[63] Study Groups are set up to support the activities of a TC for a given task. They are usually disbanded after the completion of their assignment [170].

[64] A TC can establish Working Groups that are focusing on specific tasks. They are responsible to develop the first drafts of the standards or other deliverables [170].

Note that P-members are required to participate actively in the work of the TC by voting on all official committee ballots (e.g., at various stages of standards development) as well as by participating in all the plenary meetings of the TC. In contrast, O-members can observe the standards that are being developed and contribute to the work, albeit without formal obligation. Therefore, O-members have less impact on voting results and cannot participate in any WG of the TC [147].

Figure 28: ISO/TC 307 membership [148]

5.2.2 Liaisons

In general, liaisons are established to facilitate better coordination and collaboration in the standards development processes. Depending on the nature and the type of liaison, the following distinction is typically made:

- **Outgoing liaisons:** ISO/TC 307 can access the documents of the TC in liaison and contribute to its work, through a nominated liaison officer. The liaison officer shall participate in the meetings of the TC in liaison, share the relevant documents of the TC within ISO/TC 307 (via the Secretariat), submit progress reports and coordinate inputs from experts of ISO/TC 307 on shared documents.
- **Incoming liaisons:** a TC can access the documents of ISO/TC 307 and contribute to its work, through a nominated liaison officer. The liaison officer has the same responsibilities towards her TC as liaisons officer from ISO/TC 307 in case of outgoing liaisons.
- **Bilateral liaisons:** both outgoing and incoming liaisons are established between the TCs.

Figure 29 provides an overview of ISO/TC 307's incoming, outgoing and bilateral liaisons. The liaisons formed with other ISO committees are referred as internal liaisons while the ones established with other organizations are external liaisons. ISO/TC 307 has five external liaisons with the European Commission (EC), International Federation of Surveyors (FIG), International Telecommunication Union (ITU), Society for Worldwide Interbank Financial Telecommunication (SWIFT) and United Nations Economic Commission for Europe (UNECE).

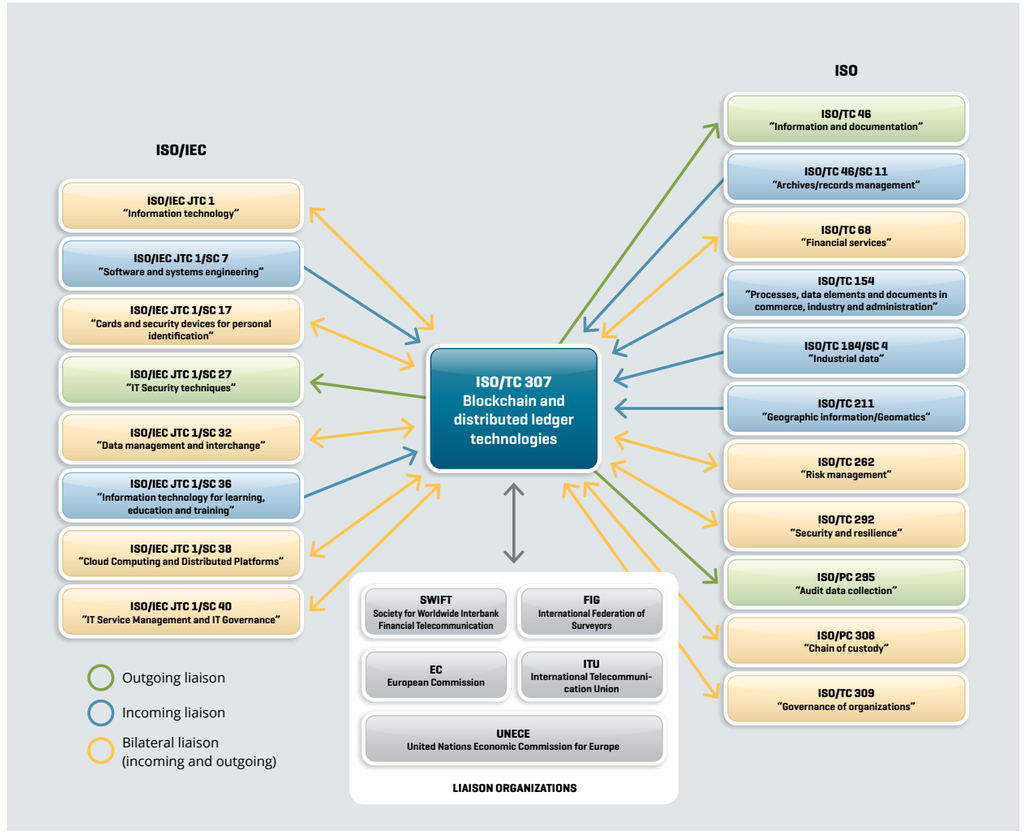


Figure 29: ISO/TC 307 liaisons [148]

5.2.3 Structure of the Committee

The ISO/TC 307 has progressively defined its structure in order to respond to the market needs and to ensure the best working environment for the success of its projects. Figure 30 illustrates the evolution of this structure since its creation and reflects the decisions (taken during the plenary meetings) that affect the TC's very structure.

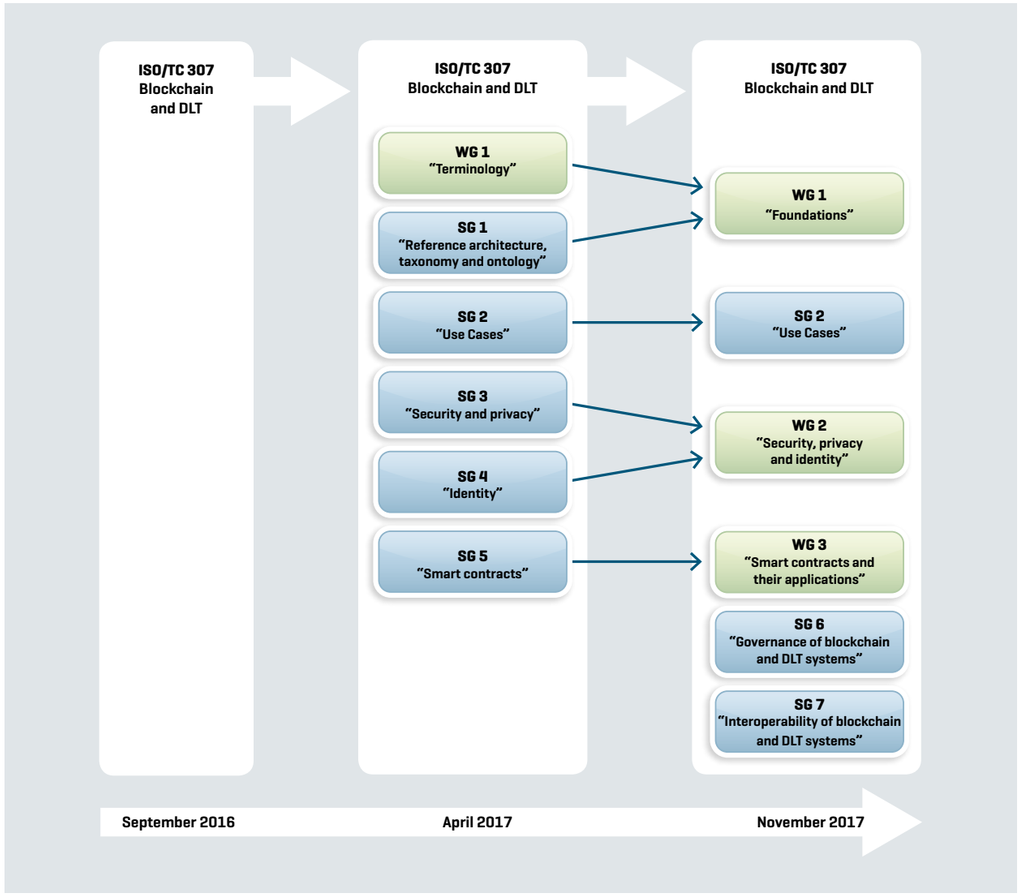


Figure 30: Evolution of ISO/TC 307 structure since its creation

ISO/TC 307 is currently composed of three Working Groups (WGs) and three Study Groups (SGs); the responsibilities of each are summarized here:

- **WG 1 Foundations:** This WG is responsible for the standardization of blockchain and DLT reference architecture, taxonomy and ontology, as well as terminology and concepts.
- **WG 2 Security, privacy and identity:** It is in charge of conducting standardization activities in the areas of security, privacy and identity of blockchain and DLT systems as well as related technologies and topics.
- **WG 3 Smart contracts and their applications:** This WG is responsible for the development of work items that relate to all aspects of smart contracts and to the complete lifecycle of DLT applications. It will also progress work items with a more focused perspective on smart contracts with a primarily legally binding intention to support documentation and operation.
- **SG 2 Use cases:** It is responsible to consider the most common types of use cases and the potential implications of the existing use cases and applications, aiming to report to ISO/TC 307 at its third plenary meeting with recommendations for future work.
- **SG 6 Governance of blockchain and distributed ledger technology systems:** This SG is in charge of studying literature on relevant topics; it is required to provide a report including recommendations and proposals to ISO/TC 307 at the third plenary meeting (May 2018).

- **SG 7 Interoperability of blockchain and distributed ledger technology systems:** It is responsible to examine five key topics related to interoperability: policy, trust and organization; transport; data syntactics; data semantics; and behavioral semantics. This SG is required to report its progress during the third ISO/TC 307 plenary meeting (May 2018) and to propose appropriate recommendations for the future work.

5.2.4 Standards under development

Given its recent creation and highly evolving domain of its work, ISO/TC 307 has not publish any standard yet. It has been focusing on studying existing relevant documentation and on defining standardization work requested by the industry. However, based on this preliminary work done by SGs, the TC has already approved seven projects, as outlined in Table 28.

Project	Topic	Scope
ISO/AWI[65] 22739	**Terminology and concepts**	ISO 22739 intends to provide fundamental terminology and definitions applicable to blockchain and DLT. This document will also describe the fundamental concepts of blockchain and DLT and the relationships between these concepts.
ISO/NP[66] TR 23244	**Overview of privacy and personally identifiable information (PII) protection**	ISO/TR 23244 will provide an overview of privacy and Personally Identifiable Information (PII) protection as they apply to blockchain and DLT systems.
ISO/NP TR 23245	**Security risks and vulnerabilities**	ISO/TR 23245 will describe security risks and vulnerabilities specific to blockchain and DLT systems.
ISO/NP TR 23246	**Overview of identity**	ISO/TR 23246 will describe an overview of identity as it applies to DLT and Blockchain systems.
ISO/AWI 23257	**Reference architecture**	ISO 23257 will specify a reference architecture for blockchain and DLT systems. The reference architecture will include concepts, architecture views, functional components, roles, activities and their relationships for blockchain and DLT.
ISO/AWI TS 23258	**Taxonomy and Ontology**	ISO/TS 23258 will specify a taxonomy and an ontology for blockchain and DLT. The taxonomy will include a taxonomy of concepts (terms), a taxonomy of blockchain and DLT systems and a taxonomy of use cases. The ontology will include classes and attributes as well as relations between concepts.
ISO/AWI TS 23259	**Legally binding smart contracts**	ISO/TS 23259 will define models, components, structures and workflows for the creation of smart contracts intended to be legally binding. This document will not give rules or recommendations for legal or legislative processes.

Table 28: ISO/TC 307 projects under development

[65] AWI means "Approved Work Item". It designates the standards development stage 20.00 in the International harmonized stage codes [169].

[66] NP means "New Project". It designates the standards development stage 10.99 in the International harmonized stage codes [169].

5.2.5 Luxembourg's ISO/TC 307 mirror committee

In Luxembourg, ILNAS – with the support of ANEC GIE – manages the ISO/TC 307 National Mirror Committee (NMC), which is the group of national delegates registered to participate in the work of this TC. Currently, eleven experts are registered and they actively participate by voting and commenting on the proposals of the TC and by participating in its international plenary meetings. ILNAS and ANEC GIE also perform a broader monitoring of blockchain and DLT standardization activities in order to remain up to date and to the inform the national stakeholders about various developments. Instructions to become an ISO/TC 307 national delegate are available here[67].

5.3 ITU-T's Focus Group on the applications of DLT

In May 2017, ITU-T created a Focus Group called the "Application of Distributed Ledger Technology" (FG DLT) with the objective of "developing a standardization roadmap for interoperable DLT-based services, taking into consideration the activities underway in ITU, other standards developing organizations, forums and groups" [149]. Several projects are already under development in different ITU-T SGs. The Telecommunication Standardization Advisory Group (TSAG) advises ITU-T SGs on developments required by the market and cooperates with other parties involved in blockchain and DLT standardization in order to avoid duplication of work (e.g., with ISO/TC 307).

ITU-T FG DLT currently has four WGs (see Table 29), which are responsible to provide deliverables (reports) on DLT related topics that will serve as a basis for the development of Recommendations[68] in ITU-T SGs [150].

ITU-T Focus Group DLT's Working Groups	Mission	Expected deliverables
WG 1 State of the Art: Ecosystem, Terms, Definitions, Concepts	Identify and introduce key elements of the DLT ecosystem (e.g., terminologies, definition, taxonomy, standardization), general concepts for DLT and related technologies, and identify and analyze standardization gaps in the DLT ecosystem	Terms & Definitions; Overview, Concepts, Ecosystem; Standardization landscape
WG 2 Applications & Services	Identify and describe DLT-based use cases, specify which DLT features are required. Highlight the competitive advantage brought by DLT to the use cases. Highlight how the use cases could benefit from a standardization effort	Horizontal Applications & Services (e.g., data usage control, identity management, security); Vertical Applications & Services (e.g., telco, fintech, supply chain, energy)
WG 3 Technology Reference Framework	Study architectural aspects of DLT including interoperability and abstract a high level technology reference framework. Provide a mapping of existing DLT platforms on the framework, and explore criteria and methods for assessment	Architectural aspects and reference framework; Overview of existing platforms and mapping to reference framework; Platform assessment criteria and methods
WG 4 Policy Reference Framework	Identify and describe relevant policy and regulatory dimensions (e.g., auditability, traceability, privacy, legal compliance) and highlight associated constraints (e.g., GDPR, lawful intercept) to the adoption of DLT-based applications and services. Provide a mapping of existing DLT platforms on the dimensions, and explore methods for assessment	Policy and regulatory dimensions and constraints for adoption of DLT-based applications; Mapping of existing DLT platforms to policy and regulatory dimensions and constraints, and assessment criteria

Table 29: ITU-T Focus Group DLT's working groups, their mission and expected deliverables [149]

In addition to this Focus Group, other SGs of ITU-T are developing Recommendations related to distributed ledgers. For instance, SG 16 "Multimedia" is preparing a Recommendation entitled **"Requirements and capabilities of decentralized ledger services"** (ITU-T Draft F.DLS) that will offer an overview of decentralized ledger services (DLS) and specify requirements and capabilities of DLS [151]. Similarly, a Recommendation with the working title **"Scenarios and capability requirements of blockchain in next generation network evolution"** (ITU-T Draft Y.NGNe-BC-reqts) is under preparation by SG 13 "Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures" [152].

Other related work from SG 17 "Security", SG 13 and SG 20 "Internet of things (IoT) and smart cities and communities (SC&C)" are presented in sections 5.5 and 5.6.

5.4 CEN-CENELEC's Focus Group on blockchain and DLT

The European Commission has shown an increasing interest in blockchain and DLT. It has taken several initiatives including establishing a liaison with ISO/TC 307, organization of a workshop on blockchain and DLT policy in September 2017, and creation of the EU Blockchain Observatory and Forum [153] in February 2018. The latter's mission is to "monitor, analyze and address the implications of blockchain developments regarding transversal issues", including interoperability and standardization [153].

To support the EC in this work, CEN and CENELEC created a Focus Group on blockchain and distributed ledger technologies (CEN-CLC FG-Blockchain-DLT) in December 2017. This Focus Group organized its kick-off meeting in January 2018 and established its terms of reference and objectives. It will currently not develop standards of its own but actively participate in the international standardization work, mainly through its liaisons with ISO/TC 307 and ITU-T FG DLT. The main objectives of this Focus Group are to [154]:

- Identify of potential specific European needs;
- Support to international standardization;
- Encourage further European participation at ISO level;
- Liaise with relevant Blockchain/DLT initiatives.

The FG will particularly work towards identifying the European specificities such as interoperability, sustainable development, security, privacy, identity, smart contracts, reference architectures and identification of use cases/ business cases. In this context, the European Commission has tasked this FG to deliver a white paper on blockchain and DLT standardization. This white paper shall highlight specific European needs (e.g., EU legislations, specific European use cases, industrial priorities, etc.) and will serve as a basis for specifying European requirements in the future international standardization developments [155].

[67] https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation/experts-normalisation.html

[68] Recommendations are the primary outcomes from ITU-T. They are equivalent to International Standards in ISO and IEC.

5.5 Standardization activities related to blockchain and digital trust

In addition to standardization developments detailed in previous sections, and particularly ISO/TC 307/WG 2 projects on security, privacy and identity, in this area in 2017, following a workshop on "Security aspects of Blockchain" organized on March 21, 2017.

As discussed in Section 5.3, ITU-T has initiated several projects to study digital trust (security, privacy, interoperability, identity etc.) aspects of blockchain and DLT. ITU-T SG 17 "Security" is carrying out this work and currently the following projects are under development.

Project identifier	Title	Scope
ITU-T Draft X.dlt-sec	Privacy and security considerations for using DLT data in Identity Management	This Recommendation provides telecom specific privacy and security considerations for using DLT data in Identity Management [156]
ITU-T Draft X.sa-dlt	Security assurance for Distributed Ledger Technology	This Recommendation provides guidance on security assurance levels for DLT. It defines DLT security assurance framework in terms of data integrity, confidentiality, communication security, and credential management. Especially, focus is given to security assurance for Proof-of-Work supporting the data integrity and for cryptography supporting the confidentiality. It defines three levels of security assurance (LoSA) of DLT. It also provides guidance concerning control technologies to be used to mitigate security threats, which are only relevant with above security aspects. It does not address assurance level for authentication and access control of DLT [157].
ITU-T Draft X.sct-dlt	Security capabilities and threats of Distributed Ledger Technology	This Recommendation provides security analysis for developing, operating or using DLT and for supporting security evaluation for the platform or service system based on DLT. It analyzes security capabilities achieved by DLT itself and also list security threats to DLT [158]
ITU-T Draft X.sra-dlt	Security architecture for Distributed Ledger Technology	The purpose of this Recommendation is to give guidance to DLT application providers and service providers to reduce security risks, improve security of their applications and services based on DLT, and make the best use of DLT to provide better applications and services [159]
ITU-T Draft X.ss-dlt	Security Services based on Distributed Ledger Technology	This Recommendation is to provide recommendation on how to deliver a DLT-based security product/service, examples of security services which can be realized based on DLT and the use cases of them [160]
ITU-T Draft X.stov	Security threats to online voting using distributed ledger technology	The purpose of this draft new Recommendation is to identify security threats to online voting using DLT based on telecommunication/ICT infrastructure. This draft new Recommendation proposes example models of online voting using DLT and focuses on security threats in online voting process on the grounds of the models [161]
ITU-T Draft X.str-dlt	Security threats and requirements for digital payment services based on distributed ledger technology	This Recommendation focuses on payment services use cases and clarifies the terminology to avoid confusion by using different terms with the same meaning or vice versa. Based on the use cases analysis, service model is described and security threats and challenges analyzed. The security requirements are provided against threats and challenges [162]

Table 30: ITU-T blockchain and DLT projects related to digital trust

5.6 Standardization activities related to blockchain and Smart ICT

As described in Section 2.6, blockchain and Smart ICT – comprising cloud computing, big data and IoT – are closely interconnected in an overall ICT ecosystem. This section presents the most relevant standardization developments within the confluence of blockchain and Smart ICT domains.

5.6.1 Cloud computing

Figure 29 highlights the bilateral liaison between ISO/TC 307 and ISO/IEC JTC 1/SC 38 "Cloud Computing and Distributed Platforms" as well as the liaison established between ISO/TC 307 and ITU. These liaisons ensure a strong collaboration between all the parties involved in blockchain standardization projects related to cloud computing. Following subsections provide details about these developments.

ISO/IEC JTC 1/SC 38 has already developed many International Standards for Cloud computing and System Oriented Architecture (SOA). It is notably interested in blockchain and DLT to examine use cases addressing data provenance and chain of custody in the context of the project ISO/IEC TR "Information technology – Cloud Computing – Framework of Trust for Processing of Multi-sourced data". It is also offering its experience to support future developments of standardization in blockchain and DLT and invite liaisons organizations in this area to consider its projects, like ISO/IEC 22624 "Information technology -- Cloud Computing -- Taxonomy based data handling for cloud services" in the context of PII protection. In addition, ISO/IEC TR "Information technology -- Cloud Computing -- Edge computing landscape" should be considered for systems using edge computing in the blockchain and DLT context.

ITU-T SG 13 "Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures" has recently started developing a Recommendation considering blockchain as a service (BaaS) in Cloud computing environments. The project identifier and title is ITU-T Draft Y.BaaS-reqts "Cloud computing - Functional requirements for blockchain as a service". In this recommendation, BaaS is defined as a Cloud service category in which the capabilities provided to the Cloud service customer are the ability of consensus, smart contract, transaction, crypto engine, block record storage, peer-to-peer connectivity and management using blockchain technologies in Cloud computing [163].

5.6.2 Internet of Things and Big Data

ISO/IEC JTC 1/SC 41 "Internet of Things and related technologies" is in charge of IoT standardization at ISO and IEC levels. It is in liaison with ISO/TC 307 and ITU-T and is currently developing projects that could be of interest for blockchain and DLT standardization. Firstly, SC 41 projects and publications on IoT vocabulary (ISO/IEC 20924), use cases (ISO/IEC TR 22417:2017) and reference architecture (ISO/IEC 30141) should be considered in blockchain use cases since many of them involve IoT devices and systems. Secondly, the projects on IoT interoperability (ISO/IEC 21823 series) should also be examined for the definition of projects in this area for blockchain and DLT.

On the other hand, ITU-T/SG 20 "Internet of things (IoT) and smart cities and communities (SC&C)" is analyzing the potential of blockchain and DLT to improve IoT/SC&C applications and services. In this context, it has launched the development of a Recommendation ITU-T Draft Y.IoT-BoT-fw "Framework of blockchain of things as decentralized service platform". This Recommendation will carry out a comparative analysis of blockchain advantages, contribute to how the blockchain-related technologies to improve the IoT/SC&C applications and services (including IoT devices, processes and data), and study and provide relevant concept, characteristics, high-level requirements, framework, capabilities and use cases [164].

ITU-T Focus Group on "Data Processing and Management to support IoT and Smart Cities & Communities" (FG-DPM) is working on the production of deliverables in the area of data processing and data management in support of ITU-T/SG 20. It is notably studying the use of blockchain related to IoT to support data management through a dedicated WG – ITU-T FG DPM/WG 3 "Data sharing, Interoperability and Blockchain" – that is responsible to study the use of blockchain in DPM. This WG is currently developing three technical reports related to blockchain:

- **Overview of IoT and Blockchain:** This technical report provides overview of blockchain aspect of the DPM for IoT and SC&C.
- **Blockchain-based Data Exchange and Sharing Technology:** This technical report provides Blockchain-based Data Exchange and Sharing Technology aspect of DPM for IoT and SC&C.
- **Blockchain Based Data Management:** This technical report provides the data management aspect study in IoT and SC&C by utilizing Blockchain technology.

5.7 Summary of blockchain and DLT standardization projects

Topic	Sub-topic	TC/WG/SG/FG	Project reference	Project title
Foundations	Terminology; Definitions; Concepts	ITU-T/FG DLT/ WG 1	(reports)	• Terms & Definitions • Overview • Concepts • Ecosystem • Standardization landscape
		ISO/TC 307/ WG 1	ISO/AWI 22739	Terminology and concepts
	Taxonomy; Ontology		ISO/AWI TS 23258	Taxonomy and Ontology
	Reference architecture; Functional requirements; Framework		ISO/AWI 23257	Reference architecture;
		ITU-T/SG 16	F.DLS	Requirements and capabilities of decentralized ledger services
		ITU-T/SG 13	Y.BaaS-reqts	Cloud computing - Functional requirements for blockchain as a service
			Y.NGNe-BC-reqts	Scenarios and capability requirements of blockchain in next generation network evolution
		ITU-T/SG 20	Y.IoT-BoT-fw	Framework of blockchain of things as decentralized service platform
		ITU-T/FG DLT/WG 3	(reports)	• Architectural aspects and reference framework • Overview of existing platforms and mapping to reference framework • Platform assessment criteria and methods
	IoT / Smart Cities	ITU-T FG DPM/ WG 3	(reports)	• Overview of IoT and Blockchain • Blockchain-based Data Exchange and Sharing Technology • Blockchain Based Data Management
Use Cases		ISO/TC 307/ SG 2	(reports)	Use cases
		ITU-T/FG DLT/ WG 2	(reports)	• Horizontal Applications & Services (e.g., data usage control, identity management, security). • Vertical Applications & Services (e.g., telco, fintech, supply chain, energy).

Digital Trust	Security	ITU-T/SG 17	X.sra-dlt	Security architecture for Distributed Ledger Technology
			X.sa-dlt	Security assurance for Distributed Ledger Technology
			X.sct-dlt	Security capabilities and threats of Distributed Ledger Technology
			X.ss-dlt	Security Services based on Distributed Ledger Technology
			X.stov	Security threats to online voting using distributed ledger technology
			X.str-dlt	Security threats and requirements for digital payment services based on distributed ledger technology
		ISO/TC 307/ WG 2	ISO/NP TR 23245	Security risks and vulnerabilities
	Privacy		ISO/NP TR 23244	Overview of privacy and personally identifiable information (PII) protection
	Identity		ISO/NP TR 23246	Overview of identity
		ITU-T/SG 17	X.dlt-sec	Privacy and security considerations for using DLT data in Identity Management
	Interoperability	ISO/TC 307/ SG 7	(reports)	Interoperability of blockchain and DLT systems
Governance		ISO/TC 307/ SG 6	(reports)	Governance of blockchain and DLT systems
Policy / Regulation		ITU-T/FG DLT/ WG 4	(reports)	• Policy and regulatory dimensions and constraints for adoption of DLT-based applications • Mapping of existing DLT platforms to policy and regulatory dimensions and constraints, and assessment criteria
Smart Contracts		ISO/TC 307/ WG 3	ISO/AWI TS 23259	Legally binding smart contracts

Table 31: Summary of blockchain and DLT standardization projects

6

Outlook and conclusions

6. Outlook and conclusions

Information and Communication Technologies are becoming essential elements of the global economy as well as today's society and life. Both public and private sectors across the world are transforming their countries and businesses with ICT programs ranging from research and innovation, infrastructure building, and skills development. One ICT innovation – namely, blockchain and distributed ledger technologies – has attracted unparalleled attention of various stakeholders across the world in the past few years.

A blockchain is a distributed ledger that allows a network of computers to jointly create, evolve and keep track of a database of records, without having a trust third party. Considering the potential of this innovation, a number of open-source platforms that not only accommodate the generalized notion of digital assets and various design choices, but also allow users to create their own decentralized applications, have been developed.

The most interesting feature of blockchain and distributed ledger technologies is that their outcomes are disruptive as well as foundational to various forms of commerce such as record keeping, contracting, clearing and settling. Consequently, their adoption is expected to trigger innovation across wide-ranging domains, and result in reduction in transaction costs, streamlining of operational processes and improve profit margins. For instance, the world of money and finance is rapidly transforming thanks to digitized assets and innovative financial channels. This transformation has accelerated with the advent of bitcoin as the first fully decentralized digital currency, creating new paradigms for financial transactions and instruments for forging alternative conduits of capital. Similarly, the ability of blockchain to ensure de facto integrity, nonrepudiation and immutability of records, facilitates secure exchange of data, which could help in reducing frauds and improving transparency and traceability.

The European Commission has launched the EU Blockchain Observatory and Forum and is studying the feasibility of an EU public blockchain infrastructure to develop cross-border services. Luxembourg is also creating an ecosystem that favors businesses of all sizes and focus areas, and is rapidly positioning itself as a leader in the fintech revolution. For instance, Luxembourg is already home to a wide range of companies and start-ups providing wealth management, payments, cryptocurrency exchange and insurance solutions, to name a few. Beyond fintech, Luxembourg is actively promoting blockchain and DLT in the areas such as identity management and data protection services, logistics and healthcare. It has also launched the Infrachain initiative to develop a trusted and compliant blockchain infrastructure that allows companies in Europe to develop enterprise-grade applications.

The rapid technological advancements as well as adoption across economic sectors have warranted a careful analysis and development of technical standards. For instance, data standards are a prerequisite to streamline supply chains and standards facilitating interoperability are of at most importance to any application where business partners need to interact in order to generate value. Similarly, availability of security and privacy standards are necessary for efficient implementation of identity management platforms. The European Commission (EC) plans to continue to appraise legal, governance and scalability issues and support interoperability and standardization efforts, including further evaluating the use of blockchain as the Next Generation Internet. The Commission has established a liaison with ISO/TC 307 in order to engage in and contribute to the development of future standards. The EC also follow the works of the ITU-T Focus Group on Application for Distributed Ledger Technologies.

In Luxembourg, ILNAS – with the support of ANEC GIE – is actively following the standardization developments of blockchain and DLT, building on the national Policy for ICT Technical Standardization (2015-2020) [69]. The main objectives of this policy are to foster and strengthen the national ICT sector's involvement in the standardization work. To achieve this, ILNAS is conducting three intertwined projects: a) developing market interest and involvement, b) promoting and reinforcing market participation, and c) supporting and strengthening the education about standardization and related research activities.

[69] https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf

In line with the first project, ILNAS and ANEC G.I.E. – in collaboration with the Ministry of the Economy – is publishing this white paper with the goal of providing a comprehensive analysis of blockchain and DLT from technological, economic and business, as well as technical standardization perspectives. Among other outcomes, this white paper aims to create awareness and interest concerning relevant standardization developments within the national market.

Similarly, conforming to the second project, ILNAS is already a P-member of ISO/TC 307 in which, 11 experts are currently building and reinforcing national participation. In addition, ILNAS is closely following the developments of ITU-T FG DLT as well as CEN/CLC FG Blockchain and Distributed Ledger Technologies, and actively transferring relevant information to the market. Interested stakeholders in Luxembourg could involve in the standards development process by becoming delegates (e.g., of ISO/TC 307)[70].

Finally, for the third project, ILNAS is strengthening its relations with the University of Luxembourg (SnT) in order to facilitate standards-related education and research. As part of this partnership, the second edition of the university certificate program "Smart ICT for Business Innovation" is currently underway. Based on the experiences from these certificate programs, ILNAS and University of Luxembourg aim to launch a full-fledged Master degree "Smart Secure ICT for Business Innovation" where digital trust and technical standardization will be at the heart of the program and be taught transversal to various Smart ICT topics, including blockchain and DLT.

These three projects will allow the national market to make rapid progress and reap the benefits of technical standardization effectively. They will also serve as a basis for ILNAS to formulate the next national Policy for ICT Technical Standardization (2020-2030) in which blockchain and DLT will be an integral part.

[70] For relevant information, visit https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation/experts-normalisation.html

References

[1] Blockchain: Powering the Internet of Value, Evry.

[2] A. Baliga, "Understanding Blockchain Consensus Models," Persistent Systems Ltd., April 2017.

[3] A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly, July 2014.

[4] J. Barrdear and M. Kumhof, "The macroeconomics of central bank issued digital currencies," Bank of England, London, 2016.

[5] "Bitcoin: Open source P2P money," [Online]. Available: https://bitcoin.org/en/. [Accessed August 2017].

[6] S. Brakeville and B. Perepa, "Blockchain basics: Introduction to distributed ledgers," IBM, May 2016. [Online]. Available: https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs/index.html. [Accessed August 2017].

[7] D. Yang, J. Gavigan and Z. Wilcox-O'Hearn, "Survey of confidentiality and privacy preserving technologies for blockchain," R3, 2016.

[8] "Impacts of the Blockchain on fund distribution," Deloitte Luxembourg, June 2016.

[9] M. Jakobsson and A. Juels, "Proofs of Work and Bread Pudding Protocols," Communications and Multimedia Security, pp. 258-272, 1999.

[10] "Proof of Work," [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_work. [Accessed August 2017].

[11] A. Kiayias, I. Konstantinou, A. Russell, B. David and R. Oliynykov, "A Provably Secure Proof-of-Stake Blockchain Protocol," September 2016.

[12] "Proof of Stake," [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_Stake. [Accessed August 2017].

[13] D. Schwartz, N. Youngs and A. Britto, "The Ripple Protocol Consensus Algorithm," Ripple Labs Inc., 2014.

[14] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 2008.

[15] P. Barron, "On Distributed Communications: Introduction to Distributed Communications Networks," August 1964.

[16] T. McConaghy, R. Marques, A. Müller, D. D. Jonghe, T. McConaghy, G. McMullen, R. Henderson, S. Bellemare and A. Granzotto, "BigChainDB: A Scalable Blockchain Database," BigchainDB, June 2016.

[17] "Blockchain proof of concept to solve traceability issues in art," Deloitte, May 2016. [Online]. Available: https://www2.deloitte.com/lu/en/pages/technology/articles/blockchain-proof-concept-solve-traceability-issues-art.html. [Accessed August 2017].

[18] E. Wall and G. Malm, "Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository," Lund University, June 2016.

[19] V. Buterin, "Ethereum white paper," 2013.

[20] A. Kosba, A. Miller, E. Shi, Z. Wen and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in Proc. of IEEE Symposium on Security and Privacy, San Jose, CA, USA, May 2016.

[21] "Interledger," [Online]. Available: https://interledger.org/. [Accessed 2017].

[22] "The Bitfury Group," [Online]. Available: http://bitfury.com/. [Accessed August 2017].

[23] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso and P. Rimba, "A Taxonomy of Blockchain-Based Systems for Architecture Design," in Proc. of 2017 IEEE International Conference on Software Architecture, Gothenburg, Sweden, April 2017.

[24] T. Swanson, "Consensus-as-a-service: A Brief Report on the Emergence of Permissioned, Distributed Ledger System," 2015.

[25] N. Atzei, M. Bartoletti and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," in Proc. of International Conference on Principles of Security and Trust, Uppsala, Sweden, March 2017.

[26] C. Cachin and M. Vukolić, "Blockchain Consensus Protocols in the Wild," eprint arXiv: 1707:01873, July 2017.

[27] "Hyperledger -- Blockchain Technologies for Business," [Online]. Available: https://www.hyperledger.org/. [Accessed August 2017].

[28] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance and Proactive Recovery,” ACM Transactions on Computer Systems, vol. 20, no. 4, pp. 398-461, 2002.

[29] S. Liu, C. Cachin and M. Vukolić, “XFT: Practical Fault Tolerance beyond Crashes,” in 12th USENIX Symposium on Operating Systems Design and Implementation, Savannah, GA, USA, November 2016.

[30] K. O’Dwyer and D. Malone, “Bitcoin mining and its energy footprint,” in Irish Signals and Systems Conference, Limerick, Ireland, 2014.

[31] “Blackcoin,” [Online]. Available: http://blackcoin.co/. [Accessed August 2017].

[32] “Nxt - The Blockchain Application Platform,” [Online]. Available: https://nxtplatform.org/. [Accessed August 2017].

[33] A. Poelstra, “Distributed Consensus from Proof of Stake is Impossible,” March 2015.

[34] D. Mazières, “The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus,” Stellar Development Foundation, February 2016.

[35] N. Szabo, “Smart Contracts: Building Blocks for Digital Markets,” Extropy, 1996.

[36] I. Bashir, Mastering Blockchain, Packt Publishing, March 2017.

[37] S. Thomas and E. Schwartz, “Smart Oracles: A Simple, Powerful Approach to Smart Contracts,” [Online]. Available: https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts. [Accessed August 2017].

[38] “Solidity,” [Online]. Available: https://github.com/ethereum/solidity. [Accessed August 2017].

[39] “Ethereum Project,” [Online]. Available: https://www.ethereum.org/. [Accessed August 2017].

[40] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang, “Untangling Blockchain: A Data Processing View of Blockchain Systems,” arXiv, pp. 1-20, August 2017.

[41] “Hyperledger (Wiki),” [Online]. Available: https://en.wikipedia.org/wiki/Hyperledger. [Accessed August 2017].

[42] C. Brett, “Hyperledger membership analysis,” September 2017. [Online]. Available: https://www.enterprisetimes.co.uk/2017/09/01/hyperledger-membership-analysis/. [Accessed October 2017].

[43] “Hyperledger Architecture, Volume 1,” Hyperledger Architecture Working Group, 2017.

[44] “Ethereum Homestead Documentation (Release 0.1),” Ethereum, March 2017.

[45] “Luxembourg Stock Exchange introduces blockchain into reporting service,” October 2016. [Online]. Available: https://www.bourse.lu/blockchain-press-release. [Accessed September 2017].

[46] J. Redman, “Jaxx: The New Fleet of Bitcoin and Ethereum Wallets,” February 2016. [Online]. Available: https://news.bitcoin.com/jaxx-the-new-fleet-of-bitcoin-ethereum-wallets/. [Accessed September 2017].

[47] “Ethereum-based Slock.it reveals first ever lock opened with money,” International Business Times UK, December 2015. [Online]. Available: http://www.ibtimes.co.uk/ethereum-based-slock-reveals-first-ever-lock-opened-money-1527014. [Accessed September 2017].

[48] “A Social Operating System for Decentralized Organizations,” Backfeed, [Online]. Available: http://backfeed.cc/. [Accessed September 2017].

[49] S. Higgins, “Why a German Power Company is Using Ethereum to Test Blockchain Car Charging,” May 2016. [Online]. Available: https://www.coindesk.com/german-utility-company-turns-to-blockchain-amid-shifting-energy-landscape/. [Accessed September 2017].

[50] “Ethereum,” [Online]. Available: https://en.wikipedia.org/wiki/Ethereum.

[51] “Ethereum (Wiki),” [Online]. Available: https://en.wikipedia.org/wiki/Ethereum. [Accessed August 2017].

[52] “Understanding Initial Coin Offerings: Technology, Benefits, Risks and Regulations,” Technology, Stellar Development Foundation and The Luxembourg House of Financial, September 2017.

[53] P. Gratzke, D. Schatsky and E. Piscini, “Signals for strategists: banding together for blockchain,” Deloitte University Press, August 2017.

[54] “The Coco Framework Technical Overview,” Microsoft, August 2017.

[55] 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,” in 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, 2017.

[56] P. Rimba, A. B. Tran, I. Weber, M. Staples, A. Ponomarev and X. Xu, “Comparing Blockchain and Cloud Services for Business Process Execution,” in IEEE International Conference on Software Architecture, 2017.

[57] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri and V. Sassone, “Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments,” in First Italian Conference on Cybersecurit, 2017.

[58] T. McConaghy, “Blockchains for Artificial Intelligence,” BigchainDB, January 2017. [Online]. Available: https://blog.bigchaindb.com/blockchains-for-artificial-intelligence-ec63b0284984. [Accessed September 2017].

[59] T. McConaghy, “Blockchains for Big Data,” BigchainDB, November 2016. [Online]. Available: https://blog.bigchaindb.com/blockchains-for-big-data-from-data-audit-trails-to-a-universal-data-exchange-cf9956ec58ea. [Accessed September 2017].

[60] A. Ekblaw, A. Azaria, J. Halamka and A. Lippman, “A Case Study for Blockchain in Healthcare: MedRec prototype for electronic health records and medical research data,” MIT Media Lab and Beth Israel Deaconess Medical Center, August 2016.

[61] N. Gupta, A. Jha and P. Roy, “Adopting Blockchain Technology for Electronic Health Record Interoperability,” Cognizant Technology Solutions, 2016.

[62] T. McConaghy and D. Holtzman, “Towards an ownership layer for the Internet,” ascribe GmbH, 2015.

[63] “We power the creative content that enlightens the Internet,” [Online]. Available: https://monegraph.com/. [Accessed September 2017].

[64] H. Es-Samaali, A. Outchakoucht and J.-P. Leroy, “A blockchain-based access control for big data,” International Journal of Computer Networks and Communications Security, vol. 5, no. 7, pp. 137-147, July 2017.

[65] E. Karafiloski, “Blockchain Solutions for Big Data Challenges,” in IEEE EUROCON, Ohrid, Macedonia, 2017.

[66] “Interplanetary Database,” [Online]. Available: https://ipdb.io/. [Accessed September 2017].

[67] A. Gantait, J. Patra and A. Mukherjee, “Implementing blockchain for cognitive IoT applications,” IBM (Developer Works), 2017.

[68] M. Conoscenti, A. Vetro and J. C. D. Martin, “Blockchain for the Internet of Things: a Systematic Literature Review,” in 13th IEEE/ACS International Conference of Computer Systems and Applications, Agadir, Morocco, 2016.

[69] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access Special section on the plethora of research in Internet of Things, vol. 4, pp. 2292-2303, 2016.

[70] A. Dorri, S. Kanhere and R. Jurdak, “Blockchain for IoT security and privacy: The case study of a smart home,” in IEEE International Conference on Pervasive Computing and Communications Workshops, Kona, HI, USA, 2017.

[71] “Filament,” 2016. [Online]. Available: https://filament.com/assets/downloads/Filament%20Foundations.pdf. [Accessed October 2017].

[72] A. Bahga and V. Madisetti, “Blockchain Platform for Industrial Internet of Things,” Journal of Software Engineering and Applications, vol. 9, pp. 533-546, 2016.

[73] ILNAS, White Paper - Digital Trust for Smart ICT, Luxembourg, 2016.

[74] X. Li, P. Jiang, T. Chen, X. Luo and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, 2017.

[75] H. Mayer, “ECDSA Security in Bitcoin and Ethereum: a Research Survey,” CoinFabrik, 2016.

[76] N. Christin, “Traveling the silk road: a measurement analysis of a large anonymous online marketplace,” in Proceedings of the 22nd international conference on World Wide Web, Rio de Janeiro, Brazil, 2013.

[77] G. Karame, E. Androulaki, M. Roeschlin, A. Gervais and S. Capkun, “Misbehavior in Bitcoin: A Study of Double-Spending and Accountability,” ACM Transactions on Information and System Security (TISSEC), vol. 18, no. 1, 2015.

[78] D. Siegel, “Understanding the DAO attack,” [Online]. Available: https://www.coindesk.com/understanding-dao-hack-journalists/. [Accessed March 2018].

[79] “King of the Ether Throne,” [Online]. Available: https://www.kingoftheether.com/postmortem.html.

[80] A. Dika, “Ethereum Smart Contracts: Security Vulnerabilities and Security Tools,” NTNU, 2017.

[81] F. Zhang, E. Cecchetti, K. Croman, A. Juels and E. Shi, “Town Crier: An Authenticated Data Feed for Smart Contracts,” in Proceedings of the ACM Conference on Computer and Communications Security, Vienna, Austria, 2016.

[82] J. Wilcke, "The Ethereum network is currently undergoing a DoS attack," [Online]. Available: https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/. [Accessed March 2018].

[83] B. Rivlin, "Vitalik Buterin on Empty Accounts and the Ethereum State," [Online]. Available: https://www.ethnews.com/vitalik-buterin-on-empty-accounts-and-the-ethereum-state. [Accessed March 2018].

[84] C. Framknecht, D. Velicanu and S. Yakoubov, "A decentralized public key infrastructure with identity retention," MIT, 2014.

[85] B. Fredriksson, "A Distributed X.509 Public Key Infrastructure Backed by a Blockchain," KTH Royal Institute of Technology, Sweden, 2017.

[86] A. Kudra, "Blockchain Comparison Criteria Catalogue," Contribution to TeleTrust working group "Blockchain", 2018.

[87] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer and S. Capkun, "Evaluating User Privacy in Bitcoin," in International Conference on Financial Cryptography and Data Security, 2013.

[88] M. Finck, "Blockchains and Data Protection in the European Union," Max Planck Institute for Innovation and Competition, 2018.

[89] J. Heng, R. Kandaswamy, N. Barton and D. Groombridge, "Market Guide for Blockchain Consulting and Proof-of-Concept Development Services," Gartner report ID: G00317612, 2017.

[90] D. He, K. Habermeier, R. Leckow, V. Haksar, Y. Almeida, M. Kashima, N. Kyriakos-Saad, H. Oura, T. Sedik, N. Stetsenko and C. Verdugo-Yepes, "Virtual Currencies and Beyond: Initial Considerations," International Monetary Fund, 2016.

[91] M. Staples, S. Chen, S. Falamaki, A. Ponomarev, P. Rimba, A. B. Tran, I. Weber, X. Xu and J. Zhu, "Risks and opportunities for systems using blockchain and smart contracts," Data61 (CSIRO), Sydney, 2017.

[92] M. Pisa and M. Juden, "Blockchain and Economic Development: Hype vs. Reality (CGD Policy Paper)," Center for Global Development, Washington DC, 2017.

[93] "Understanding the landscape of Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards," British Standards Institution, London, 2017.

[94] V. Espinel, D. O'Halloran, E. Brynjolfsson and D. O'Sullivan, "Deep Shift: Technology Tipping Points and Societal Impact (Survey Report)," World Economic Forum, 2015.

[95] "Global Opportunity Report," DNV GL AS, 2017.

[96] M. Kashyap, J. Shipman, H. Garfinkel, S. Davies and D. Nicolacakis, "Redrawing the lines: FinTech's growing influence on Financial Services," PwC, 2017.

[97] "Coin Dance Statistics," [Online]. Available: https://coin.dance/stats. [Accessed February 2018].

[98] G. Hileman and M. Rauchs, "Global Cryptocurrency Benchmarking Study," Cambridge Centre for Alternative Finance and Visa, Cambridge, UK, 2017.

[99] "Coindesk ICO Tracker," [Online]. Available: https://www.coindesk.com/ico-tracker/. [Accessed February 2018].

[100] B. Fung and H. Halaburda, "Central Bank Digital Currencies: A Framework for Assessing Why and How," Bank of Canada, 2016.

[101] S. Takagi, "The Impact of Central Bank Digital Currency: From a Functional Perspective," Center for Global Communications, International University of Japan, Discussion Paper Series 17-003, 2017.

[102] "Top 10 Trends in Payments," Capgemini, 2017.

[103] R. Jesse McWaters, "The future of financial infrastructure - An ambitious look at how blockchain can reshape financial services," World Economic Forum and Deloitte, 2016.

[104] "OpenBazaar," [Online]. Available: https://www.openbazaar.org/. [Accessed February 2018].

[105] P. Rizzo, "A new version of OpenBazaar is just months away," February 2017. [Online]. Available: https://www.coindesk.com/blockchain-e-commerce-openbazaar-just-months-away/. [Accessed February 2018].

[106] M. Iansiti and K. Lakani, "The truth about blockchain," Harvard Business Review, January-February, 2017.

[107] "How blockchain technology could transform the food industry," December 2017. [Online]. Available: http://theconversation.com/how-blockchain-technology-could-transform-the-food-industry-89348. [Accessed February 2018].

[108] Y. P. Lin, J. R. Petway, J. Anthony, H. Mukhtar, S. W. Liao, C. F. Chou and Y. F. Ho, "Blockchain: The Evolutionary Next Step for ICT E-Agriculture," Environments, vol. 4, no. 3, 2017.

[109] "Distributed Ledger Technology: beyond block chain," Report by the UK Government Chief Scientific Adviser, Government Office for Science, London, 2016.

[110] "e-estonia," [Online]. Available: https://e-estonia.com/solutions/e-identity/id-card/. [Accessed February 2018].

[111] "Smart Dubai," [Online]. Available: http://smartdubai.ae. [Accessed February 2018].

[112] "uport.me -- open identity system for the decentralized web," [Online]. Available: https://www.uport.me/. [Accessed February 2018].

[113] "Embracing Innovation in Government Global Trends," in World Government Summit, Organisation for Economic Co-operation and Development Publishing, Dubai, UAE, 2017.

[114] M. Swan, Blockchain blueprint for a new economy, O'Reilly Media, 2015.

[115] V. Gupta, Internet of Agreements, London: Hexayurt Capita (internetofagreements.com), 2017.

[116] D. Tapscott and A. Tapscott, The impact of the blockchain goes beyond financial services, Harvard Business Review, 2016.

[117] D. Tapscott and A. Tapscott, "How Blockchain Will Change Organizations," MIT Sloan Management Review, vol. 58, no. 2, 2017.

[118] "Association of the Luxembourg Fund Industry (ALFI)," [Online]. Available: www.alfi.lu. [Accessed 2018].

[119] "Europe's fund expenses at a crossroads: The benefits of mutualizing the cost of distribution," Fundsquare and Deloitte, Luxembourg, 2014.

[120] "How can Fintech facilitate fund distribution?," Deloitte and ALFI, Luxembourg, 2016.

[121] "Fundchain," [Online]. Available: http://fundchain.lu/. [Accessed 2018].

[122] "FundsDLT," [Online]. Available: https://www.fundsdlt.net/. [Accessed 2018].

[123] "Distributed Ledger Technology: The genesis of a new business model for the asset management industry," Fundchain and PwC, Luxembourg, 2017.

[124] "Fundsquare," [Online]. Available: https://www.fundsquare.net/. [Accessed 2018].

[125] "Unlocking Economic Advantage with Blockchain: A guide for asset managers," Oliver Wyman and JP Morgan, 2016.

[126] M. Petersen, N. Hackius and B. v. See, "Mapping the Sea of Opportunities: Blockchain in Supply Chain and Logistics," Kühne Logistics University, 2017.

[127] M. Auboin, "Improving the availability of trade finance in developing countries: an assessment of remaining gaps," World Trade Organization - Economic Research and Statistics Division, 2015.

[128] "Blockchain in logistics," DHL Trend Research, 2018.

[129] T. Groenfeldt, "IBM and Maersk apply blockchain to container shipping," [Online]. Available: https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#10bbaae43f05. [Accessed March 2018].

[130] J. Groenewegen, M. Heijmerikx and J. Kalf, "The impact of blockchain on trade finance (Economic report)," RaboResearch - Economic Research (Rabobank), [Online]. Available: https://economics.rabobank.com/publications/2017/november/the-impact-of-blockchain-on-trade-finance/. [Accessed March 2018].

[131] S. Chatterjee, V. Singla and M. Lam, "How blockchain can reshape trade finance," Deloitte.

[132] A. Beije and J. Jullens, "A lead via Blockchain technology - Position paper on a digital Port of Rotterdam," Commissioned by City of Rotterdam, 2016.

[133] "STATEC -- Luxembourg: Special NACE Rev. 2 aggregates, 2005--2015 (Structural business statistics)," [Online]. Available: http://www.statistiques.public.lu/stat/TableViewer/tableViewHTML.aspx?ReportId=13331&IF_Language=en&IF_SearchString=logistique&IF_SearchProperties=1,6&IF_SearchExactWord=true&IF_SearchType=AND&IF_SearchRange=SHARED. [Accessed April 2018].

[134] "Enabling trade valuing growth opportunities," World Economic Forum, 2013.

[135] "A Blueprint for Digital Identity - The Role of Financial Institutions in Building Digital Identity," World Economic Forum, 2016.

[136] S. Kavadias, K. Ladas and C. Loch, "The transformative business model," Harvard Business Review, October 2016. [Online]. Available: https://hbr.org/2016/10/the-transformative-business-model. [Accessed April 2018].

[137] "Personal Data: The Emergence of a New Asset Class," World Economic Forum, 2011.

[138] European Parliament and the Council, "Regulation (EU) No 1025/2012 of the European Parliament and of the Council," 2012. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF.

[139] ILNAS, "Standards Analysis Smart ICT - Luxembourg," 2018. [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/publications/normalisation/2018/standards-analysis-smart-ict-2-0.pdf.

[140] European Commission, "Europe 2020 Flagship Initiative, Innovation Union, COM(2010) 546," 2010. [Online]. Available: https://ec.europa.eu/research/innovation-union/pdf/innovation-union-communication_en.pdf.

[141] "Luxembourg Standardization Strategy 2014-2020," ILNAS, [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/strategie-normative-2014-2020/luxembourg-standardization-strategy-2014-2020.pdf.

[142] "Policy on ICT technical standardization (2015-2020)," ILNAS, [Online]. Available: https://portail-qualite.public.lu/content/dam/qualite/fr/publications/normes-normalisation/orientations-strategiques/politique-luxembourgeoise-pour-la-normalisation-technique-des-tic-2015-2020/policy-ict-technical-standardization-2015-2020.pdf.

[143] Standards Analysis - Smart ICT version 2.0, Luxembourg: ILNAS, January 2018.

[144] Standards Australia, "Roadmap for Blockchain Standards," 2017. [Online]. Available: http://www.standards.org.au/OurOrganisation/News/Documents/Roadmap_for_Blockchain_Standards_report.pdf.

[145] ISO/TC 307, N68 RESOLUTIONS MEETING 001 TC 307 FINAL, 2017.

[146] ISO/TC 307, "N194 Meeting 02 Resolutions Final," 2017.

[147] ISO/IEC, "ISO/IEC Directives, Part 1 - Consolidated ISO Supplement — Procedures specific to ISO," 2017. [Online]. Available: https://isotc.iso.org/livelink/livelink/fetch/2000/2122/4230450/4230452/ISO_IEC_Directives_Part_1_and_Consolidated_ISO_Supplement_%2D_2017_%288th_edition%29_%2D_PDF.pdf?nodeid=18905271&vernum=-2.

[148] ISO, "ISO/TC 307 Blockchain and distributed ledger technologies," [Online]. Available: https://www.iso.org/committee/6266604.html.

[149] ITU, "Focus Group on Application of Distributed Ledger Technology," [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx.

[150] ITU-T FG DLT, Overview of FG DLT working groups and deliverables.

[151] ITU-T, "F.DLS - Requirements and capabilities of decentralized ledger services," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14071.

[152] ITU-T, "Y.NGNe-BC-reqts - Scenarios and capability requirements of blockchain in next generation network evolution," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14282.

[153] European Commission, "Tender Specifications - European Blockchain Observatory and Forum - Setting-up and running a European expertise hub on blockchain and DLT - Smart 2017/1130," 2017. [Online]. Available: http://ec.europa.eu/information_society/newsroom/image/document/2017-29/smart_2017-1130_tender_specifications_C3FFB185-C346-C9FD-A79D76E0F72D4742_46087.pdf.

[154] CEN-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies, Terms of reference, 2018.

[155] CEN-CENELEC Focus Group on Blockchain and Distributed Ledger Technologies, CEN-CENELEC – Blockchain and DLT Stakeholder Engagement Workshop - White Paper project kick-off meeting, 2018.

[156] ITU-T, "X.dlt-sec - Privacy and security considerations for using DLT data in Identity Management," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14375.

[157] ITU-T, "X.sa-dlt - Security assurance for Distributed Ledger Technology," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14376.

[158] ITU-T, "X.sct-dlt - Security capabilities and threats of Distributed Ledger Technology," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14373.

[159] ITU-T, "X.sra-dlt - Security architecture for Distributed Ledger Technology," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14371.

[160] ITU-T, "X.ss-dlt - Security Services based on Distributed Ledger Technology," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14374.

[161] ITU-T, "X.stov - Security threats to online voting using distributed ledger technology," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14377.

[162] ITU-T, "X.str-dlt - Security threats and requirements for digital payment services based on distributed ledger technology," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14372.

[163] ITU-T, "Y.BaaS-reqts - Cloud computing - Functional requirements for blockchain as a service," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14485.

[164] ITU-T, "Y.IoT-BoT-fw - Framework of blockchain of things as decentralized service platform," [Online]. Available: https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14099.

[165] G. Wood, "Ethereum: A Secure Decentralized Generalised Transaction Ledger (Revision EIP-150)," April 2017.

[166] J. Douceur, "The Sybil Attack," in International Workshop on Peer-To-Peer Systems, 2002.

[167] BSI, "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards," 2017. [Online]. Available: https://www.bsigroup.com/PageFiles/508003/BSI_Blockchain_DLT_Web.pdf.

[168] China Blockchain Technology and Industrial Development Forum, "White Paper on China Blockchain Technology and Application Development," 2016.

[169] ISO, "International harmonized stage codes," [Online]. Available: https://www.iso.org/stage-codes.html.

[170] ISO, "My ISO job - What delegates and experts need to know," 2016. [Online]. Available: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/my_iso_job.pdf.

[171] ILNAS, "Certificat universitaire « Smart ICT for Business Innovation »," [Online]. Available: https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/projets-phares-dans-l_education-a-la-normalisation.html.

[172] ILNAS, "Programme de recherche ILNAS-UL : Normalisation technique pour une utilisation fiable dans le domaine « Smart ICT »," [Online]. Available: https://portail-qualite.public.lu/fr/normes-normalisation/education-recherche/programme-recherche.html.

June 2018 · Blockchain and Distributed Ledgers V1.0 · © ILNAS/ANEC

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

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