

CAS Report

Blockchain Standardization - Overview of Current Activities Landscape

CAS Big Data and Machine Learning

08.06.2020

by Luciana Cristea, General Electric

Supervisor:
Prof. Dr. Burkhard Stiller

Department of Informatics
University of Zurich



University of
Zurich ^{UZH}

Abstract

The blockchain term is being more and more visible in posts on social media websites, research papers, studies, and use cases published by companies or individuals from different areas to not miss the benefits of this innovation. However, for non-technical individuals it is time consuming to really understand what a blockchain is, its technical details, and use-cases, often leading to more questions than answers. This can be due to two main reasons (i) the contrast between opinions and definitions, and (ii) the lack of standards or guidelines available that one can use to easily navigate through the blockchain field. Therefore, having a regulatory framework suitable to deal with blockchain related business models is essential for a proper understanding and successful adoption at large scale. In this sense, this report presents an overview on the current blockchain standardization initiatives to help clarify this novel solution.



Contents

ABSTRACT.....	I
1. INTRODUCTION.....	1
1.1. WHAT IS DISTRIBUTED LEDGER?	1
1.2. WHAT IS BLOCKCHAIN?.....	2
1.3. EVOLUTION OF BLOCKCHAIN	2
1.4. NEED FOR STANDARDIZATION	3
1.5. REPORT ORGANIZATION.....	3
2. BLOCKCHAIN STANDARDIZATION LANDSCAPE.....	3
2.1. INTERNATIONAL ORGANIZATIONS	4
2.2. REGIONAL ORGANIZATIONS.....	8
3. COMPARISON OF SELECTED CHARACTERISTICS.....	9
3.1. PERMISSIONLESS VS. PERMISSIONED	9
3.2. UNDERSTANDING THE DIFFERENCES	10
4. LANDSCAPE AND CHARACTERISTICS.....	11
4.1. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO).....	11
4.2. THE INTERNATIONAL TELECOMMUNICATION UNION (ITU).....	12
5. DISCUSSION ON THE CONSENSUS	15
5.1. AGREEING ON TERMINOLOGY	15
5.2. SMART CONTRACTS.....	15
5.3. PRIVACY AND PII FOR BLOCKCHAIN/DLT SYSTEMS	16
6. CONCLUSIONS.....	17
APPENDIX A - ISO WORK STRUCTURE	18
APPENDIX B - ITU WORK STRUCTURE.....	20
APPENDIX C - ISO AND ITU CONSENSUS	24
REFERENCES.....	27

1. Introduction

Many consider that the first reference to blockchain as a cryptographically secured and chronological chain of hashed data has been introduced for the first time almost 30 years ago by Stuart Haber and W Scott Stornetta [1], as a method to timestamp a digital document. However, the first model for a blockchain and its implementation has been released only 17 years after, in 2009, with the deployment of Bitcoin [2][3]. Since then, the blockchain technology as a distributed ledger has known continuous progress, evolving beyond its (crypto)currency initial purpose and having the potential to revolutionize the way how economy works.

1.1. What is Distributed Ledger?

The concept of ledger is not new; it was already used since long time in connection with double entry booking or lately with spreadsheets as a system used to keep track of financial transactions or records. However, distributed ledger is a new, more efficient and secure way to refer to a ledger. Simply described, a distributed ledger can be viewed as a database that is replicated across multiple nodes, each node holding an identical copy of the ledger [4]. One of the main characteristics of a distributed ledger is that, in contrast with traditional databases which are managed centrally by a Trusted Third Party (TTP), it can operate without unnecessary intermediates, it is more secure and offers transparency (see Fig. 1.1) [6]. Distributed Ledger Technology (DLT) is considered highly secure because none of the nodes has central authority and as a consequence there is no single point of fraud or vulnerability in this network.

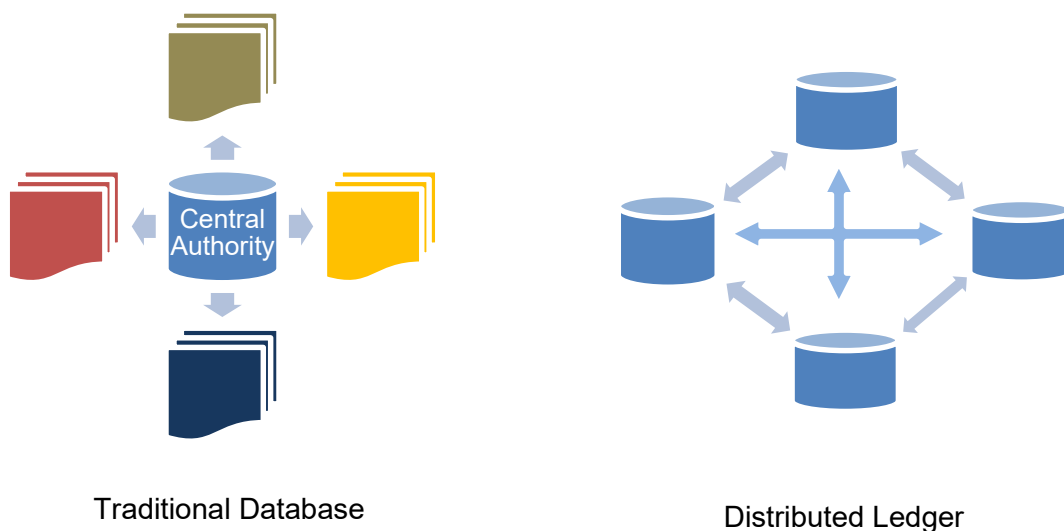


Figure 1.1: Visualisation of traditional database and distributed ledger

Transactions created in the ledger are recorded by each node independently but they are included in the ledger only when an agreement, called consensus, has been reached between participating nodes. At that moment, transactions are added on the distributed ledger and a new, agreed version of the ledger (or block) is saved on each node separately [5]. Ultimately, each node will have the updated ledger stored, resulting in consistent results.

1.2. What is Blockchain?

There is a general misunderstanding that blockchain and DLT are referring to the same concept, but in reality, that is not quite accurate. Blockchain is a type of DLT that is operated in a Peer-to-Peer (P2P) network where all nodes are equally important and are able to perform the same tasks [5]. Its structure consists of a sequence of records organized in blocks (see Figure 1.2). Blocks are added in the chain when the consensus is reached and are logically linked to each other. A block can consist of several transactions which, when added to the block, are timestamped and receive for security a unique cryptography signature. Blocks are immutable meaning that the blockchain allows only to add data (*i.e.*, append-only). Changing or deleting existing data is not possible and this makes the entire process not only fully transparent, but also verifiable and auditable for any interested peer in the network [6].

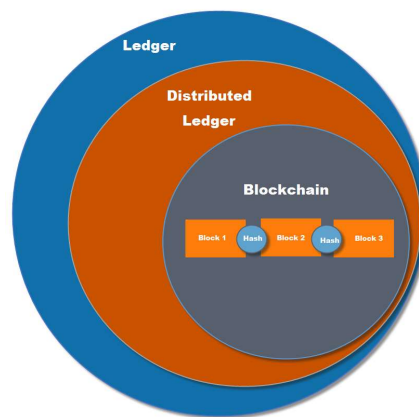


Figure 1.2: Visual representation of blockchain as one type of distributed ledger

What makes blockchain different from other types of distributed ledgers is its public nature, allowing everyone to read and write transactions or participate into consensus. Because of this blockchain is known as a public permissionless network, in contrast with permissioned networks where the rights to write transactions or participate into consensus are restricted to authorized and predefined stakeholders [40].

1.3. Evolution of Blockchain

As shortly mentioned at the beginning of this chapter, the introduction to a similar concept to the blockchain as a cryptography-based database has been done in 1991 by Stuart Haber and W Scott Stornetta in their research paper "How to Timestamp a Digital Document" [1][7]. For the following 15 years there were few attempts to develop this theoretical framework but no significant steps were made until 2008, when developer(s) working under the pseudonym Satoshi Nakamoto introduced in the white paper "Bitcoin: A Peer-to-Peer Electronic Cash System" [3]. It proposed the notion of Bitcoin currency and use it to launch, in 2009, the first blockchain as a public distributed ledger based on Bitcoin transactions [7]. The implementation of blockchain as the underlying technology for Bitcoin was just a first step towards the blockchain digital transformation.

In the last 10 years it became more and more obvious that there is an increasing need to operate efficiently and secure. Cost can be substantially minimized by eliminating intermediaries or

administrative work, and blockchain can ensure through its architecture that no central authority is needed to operate within its network. In addition, immutability can guarantee as well that data remains protected against malicious attacks, reducing the risk of data being compromised or stolen. That is why, in the last decade many efforts have been done to extend the capabilities of blockchain to build new kinds of applications with native trust, immutability and value exchange and solutions such as Ethereum, Hyperledger Fabric or Ripple have appeared and gained popularity with developers, investors or industries utilizing these systems on their networks. At the same time, each solution was trying to address to certain industries or satisfy particular needs and built up different protocols while fundamental pillars remained the same. This is how permissioned blockchain has appeared as an alternative to the traditional permissionless public networks and different variations of those have been implemented by one solution or another in this space.

1.4. Need for Standardization

All these developments increased the complexity behind blockchain and on the same time reduced the ability of the experts to fully understand the different algorithms or protocols available. In this context, any existing or future emerging market or its players must invest significant efforts in understanding not only the possible benefits of this technology but also the related risks and how these can be minimized or even eliminated.

It becomes more and more clear that blockchain technology is not yet ready to be used in critical services (e.g., healthcare or support banking) and it requires more time to mature. Blockchain technology is currently unregulated, resulting in legal ambiguities and grey areas which can easily open the door for malicious activities. According to an IBM presentation [8], 41% of organizations believe the lack of standards is the major challenge to move towards a blockchain proof of concept.

1.5. Report Organization

The remainder of this report is structured as follows. Chapter 2 introduces the current landscape on standardization of blockchain and DLT. Then, Chapter 3 compares selected characteristics from these two concepts. Chapter 4 discusses the described landscape and characteristics. Chapter 5 presents if a consensus exists between the main standardization groups. At closure, the report concludes with final remarks.

2. Blockchain Standardization Landscape

Fortunately, there are global initiatives in charge to define standards for blockchain and DLTs and as of today a number of those groups have made progress with their efforts.

The action of standardization was justified not only by the lack of governance but also by the clear expectation of participants in this industry to be able to employ this innovation with higher confidence and clarity. New standards will make possible for blockchain interoperability (*i.e.*, communication between different blockchain and DLT platforms) to come one step closer to reality. According to IBM [8], 83% of organizations believe that the existence of standards and governance will enable different types of blockchain networks to connect and work together and as a result, allow potential players to widely join them.

Furthermore, the new standards need to consider the existing global regulations and try to adapt to the existing international laws. This represents already a big challenge as they were not written to have blockchain in scope. In case of the European General Data Protection Regulation (GDPR), for example, the immutability comes in conflict with the rights of individuals to control their data – to correct, to be forgotten or to restrict data usage. GDPR enforces as well the responsibility of companies to conform and agree to limit the data transfer between countries, but on public blockchain the data is processed by many parties, anywhere [8]. Last but not least, the new United States (US) “EARN IT” act evaluates the prohibition of the end-to-end encryptions in order to “prevent terrorism” and this is as well conflicting with the principle of anonymous transfer of money which defines blockchain networks [8].

That is why, one of the current main priorities is to make sure that the standards created will be flexible enough, broadly applicable and meet the governments and private sector’s needs or adapt to them whenever needed. At the same time, most of the laws are not absolute. In case of data protection, authorities have already suggested that immutability is not necessarily a show-stopper and the technology experts found solutions to store personal data off-chain. Collaboration between players at all levels is imperative and creating or extending laws, regulations, policies or agreements becomes a necessity not only for and between organizations but also between countries at international scale [8]. The next sections describe these efforts at international and regional level.

2.1. International Organizations

Three bodies are responsible for the planning, development and adoption of International Standards: ISO (International Organization for Standardization) is accountable for all industries apart from electrotechnical industries, which are the responsibility of the International Electrotechnical Committee (IEC), and majority of telecommunications technologies industries, which are mainly under the responsibility of International Telecommunication Union (ITU).

International Organization for Standardization (ISO) is the most known independent, non-governmental global body for developing international standards.

In 2016, at the proposal of Standards Australia, ISO created a Technical Committee (TC 307) in charge with the standardization of blockchain and DLTs. In April 2017, as part of the first plenary that took place in Sydney, ISO made known the roadmap for the TC 307 development for the coming 36 months (see Figure 2.1) [9].

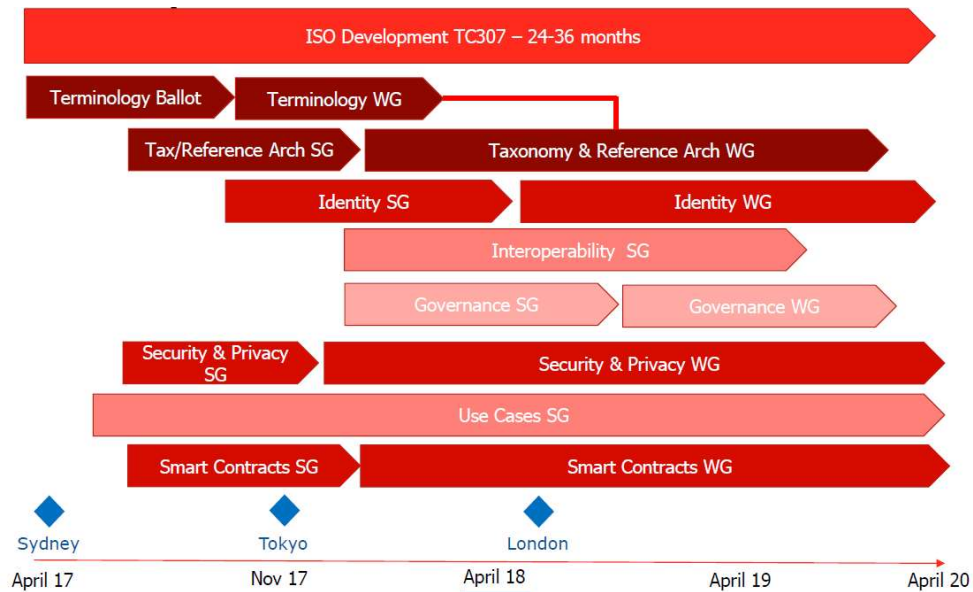


Figure 2.1: ISO Development TC 307 – 34-36 months [9]

The initial plans were very ambitious and by April 2020, all topics in the scope of the TC 307 should have been addressed and some finalized. However, at the due date, only two standards, ISO/TR 23455: 2019, related to “*Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*” and ISO/TR 23244 “*Privacy and personally identifiable information protection considerations*” have been published. Another standard, ISO/DIS 22739 “*Blockchain and distributed ledger technologies — Terminology*” is currently under preparation for its final publication and seven others are still in work having different stages of maturity [10].

Until now, six plenary meetings of TC took place and two additional meetings are being planned for 2020 and 2021 (see Figure 2.2).

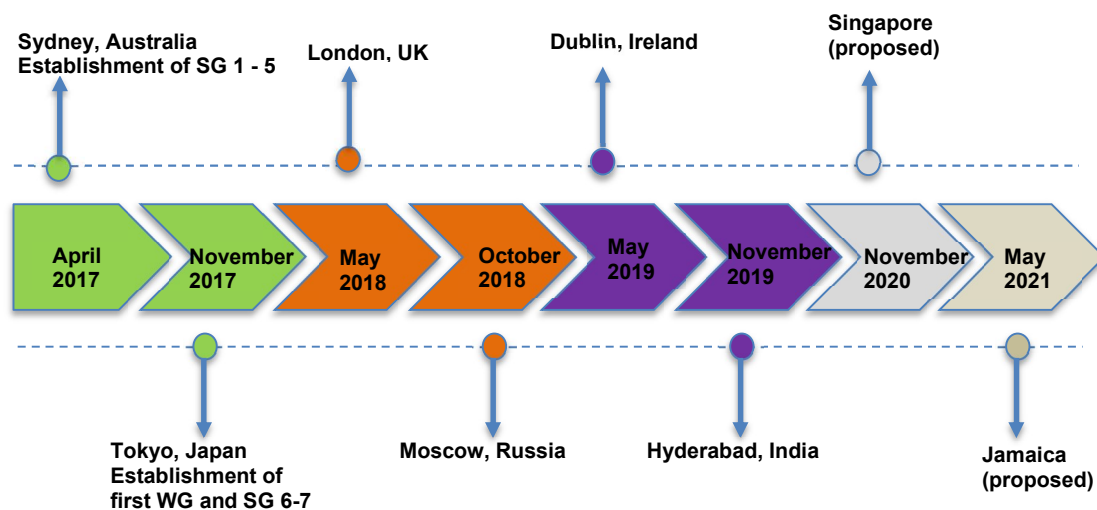


Figure 2.2: Timeline to date of ISO/TC 307 related meetings [12], [13]

As of June 2020, there are 44 participating members, 13 observing members and 11 organizations in liaison contributing to this initiative (see Appendix A.1 for details). Working Groups (WG) consist

of a limited number of experts in charge to resolve specific tasks assigned to the group. Several Advisory Groups (AG) and Study Groups (SG) are used as enablers for TC 307. They are responsible to provide guidance and recommendations or assess the viability of an idea or project. In addition, ISO is also very closely collaborating with IEC on all subjects related to electrotechnical standardization. There is already a joint working group, JWG4: Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG, addressing the blockchain and DLTs and IT Security techniques, where the two organizations are involved together. At the same time, ISO facilitates the cooperation within different ISO TCs which might discuss the same topics or have synergies.

The work around blockchain and DLTs standardization is organized in five key groups whose priorities are focused on following areas of reference [10]:

- Foundations,
- Privacy, security and identity,
- Smart contracts and their application,
- Use cases, and
- Governance.

The International Telecommunication Union (ITU) is an agency of United Nations focussed on topics related to telecommunications, Information and Communication Technologies (ICTs). It has a permanent Telecommunication Standardization Sector (ITU-T) in charge to study technical, operating and tariff questions and issue recommendations on them, explicitly on global standardizing telecommunications.

ITU-T is organized in several focus groups. One of those has been created in May 2017 and is dedicated to Application of Distributed Ledger Technology (FG DLT). FG DLT was established to [19]:

- to investigate and study DLT-based applications and services;
- to outline the best practices and provide guidance for the implementation of those applications and services on a global scale; and
- to recommend a solution for associated standardization work in ITU-T Study Groups.

FG DLT conducted seven meetings until 1st of August, 2019 (see Figure 2.3 and Table 1 from Appendix B for details), when it submitted its deliverables to its parent group, Telecommunication Standardization Advisory Group (TSAG).

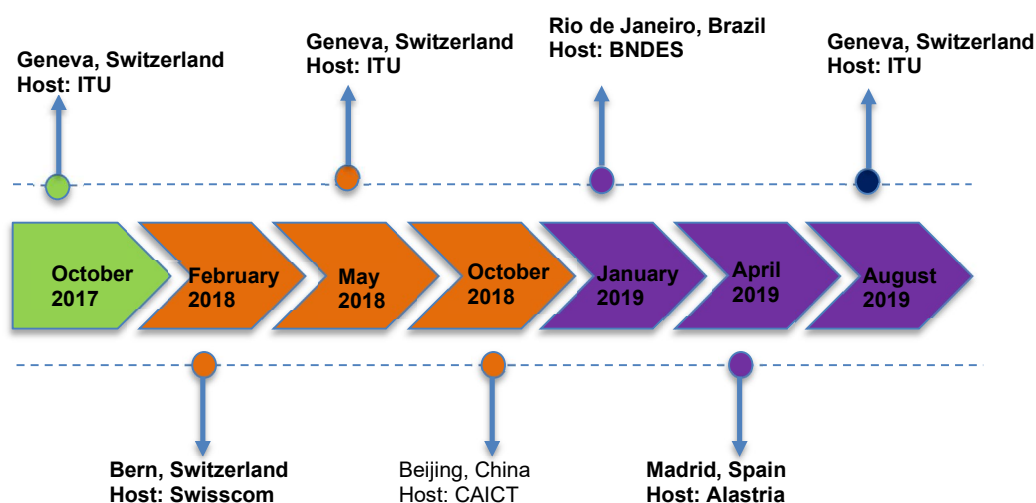


Figure 2.3. Timeline of ITU related meetings [20]

FG DLT has split its work within five working groups. In order to progress faster with their work all working groups made use of remote meeting facilities. The participants representing 38 countries and several organizations delivered three technical specifications and five technical reports focused on [20]:

- DLT terms and definitions (D1.1),
- DLT overview, concepts, ecosystems (D1.2),
- DLT standardization landscape (D1.3),
- DLT use cases (D2.1),
- DLT reference architecture (D3.1),
- Assessment criteria for DLT platforms (D3.3),
- Distributed ledger technology regulatory framework (D4.1),
- Outlook on distributed ledger technologies (D5.1).

The Internet Research Task Force (IRTF) focuses on long term research related to the application architecture and technology of internet protocols. The work of IRTF is based on the contribution of fourteen Research Groups. One of this groups is studying the Decentralized Internet Infrastructure (DINRG) and has been launched in September, 2017 [29].

DINRG is an open forum based on the collaboration by using regularly the open mailing list and occasionally by meeting physically during the year as well. The main objectives of DINRG are to [30]:

- understand, document and survey existing applications and their characteristics in the context of their implementation in a distributed manner;
- investigate solutions and how they address Internet level deployment issues related to security, performance and scalability;
- record and detail best practices and technical solutions;
- create instruments and performance indicators in order to recognize scaling problems or missing elements;
- define and propose work items for the Internet Engineering Task Force (IETF), whose work concentrates on making standards and the short-term resolution of engineering issues.

Since it has been launched, this forum had several meetings (four in 2018, two in 2019 and one in 2020). During these reunions there were several discussions around DLTs and blockchain starting with a research on blockchain as an auditable communication channel (successfully implemented with Bitcoin, Ethereum or Hyperledger Fabric), continuing with studying how distributed ledger can be applied to IoT and analysing several use cases such as Chainspace (a scalable smart contracts platform), Coconut (a scheme for selective disclosure credentials) or Interplanetary File System (IPFS) as Platform for Decentralized Applications [31]. In addition, in the last session which took place in April, 2020 a new initiative has been introduced: Blockchain Governance Initiative Network (BGIN). BGIN was launched on March 10, 2020 as a global network of engineers, regulators, academia, industry representatives as well as internet pioneers and expert groups whose main scope is understanding in detail issues and collaborate to support the sustainable extension of the blockchain community [32]. The DINRG meeting from April, 2020 was considered preparatory for the next BGIN events planned to take place in Autumn 2020 (1st BGIN meeting “BGIN Block 01”) and early 2021 (2nd BGIN meeting “BGIN Block 02”). It will be interesting to follow up on this initiative and see how it will contribute to the DLT and blockchain standardization.

The World Wide Web Consortium (W3C) is a non-profit international community with 429 members which develops Web standards [33]. In 2016, W3C has initiated a Blockchain Community Group (BCG) whose scope was to issue [34]:

- message format standards of blockchain based on ISO20022 and

- recommendations on how to use storage including torrent, public blockchain, private blockchain, side chain and Content Delivery Network (CDN)

In addition, the group proposed to study and assess blockchain related technologies as well as associated use cases.

In total, 216 people participated between March, 2016 to November 2017 to several discussions about how blockchain fits to Web technologies, what part of the Web would be impacted by its usage and if there is a need to update web protocols, formats or APIs to enable the data transactions in the scope of blockchain networks. Furthermore, several use cases have been exploited to better answer these questions. Unfortunately, after November, 2017 there is no official information about the work progress of this community. Thus, it is unknown what is the current status of their standardization efforts.

2.2. Regional Organizations

There are as well regional and local organizations which are part of the global landscape around DLTs and blockchain.

Standards Australia is an independent, non-profit and non-governmental organization having a significant impact in the global blockchain standardization. It is actually the forum which submitted, in 2016, the proposal to ISO to consider the extension of its standardization efforts to include blockchain and DLTs, which provided the basis of ISO/TC 307, Blockchain and Distributed Ledger Technologies. Standards Australia hosted in February 2017 the first ISO workshop in Sydney and proposed the key priorities and the Roadmap Blockchain Standards Report [35].

The Australian government provided 350'000 USD to Standards Australia to lead the blockchain international standardization [36]. This high interest is justified by the fact that Australia is, on one side, pioneer in a number of blockchain applications and, on the other side, ranked six internationally in blockchain related patent fillings. The government understood that in order to support the technology to mature it is crucial to enable the development of common standards.

Standards Australia had as well an important contribution to the ISO's first technical report published in September 2019: ISO/TR 23455:2019 "*Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*". By using smart contracts, commodities can be moved across border faster and more secure supporting in an innovative way the Australian export, which is crucial for its economy.

CEN-CENELEC: The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC) have a 60 years' contribution to the European standardization. As a result of a common initiative, a Focus Group on Blockchain and Distributed Ledger Technologies (DLT) has been created in 2017 [37]. Its objective was to understand the industry and identify what standardization activities are necessary, what proposals have to be made and what actions have to be initiated by policy makers, between regulations and standardization. The first milestone has been achieved and the findings have been published in the CEN-CENELEC White Paper "*Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies*" [38]. The report describes opportunities as well as challenges and proposes the way forward for CEN-CENELEC. Future activities should consider models that support smart contracts or enable interoperability between different platforms but the extension or adaption of current legal and regulatory framework as well.

Recently, the CEN-CENELEC has released the work programme for 2020 [39]. During this year, the aim of the joint committee will be to address specific European requirements with focus on legislative and policy context, while considering the adoption of existing or in work standards. The plan is to set up two specific working groups on Electronic Identification, Authentication and Trust Services (eIDAS) and GDPR, which will require strong cooperation with other CEN-CENELEC initiatives in the area of *“Personal identification and related personal devices with secure elements, systems, operations and privacy”* (CEN/TC 224) and *“Cybersecurity and data protection”* (CEN-CLC/JTC 13).

3. Comparison of Selected Characteristics

Before discussing more in detail about the landscape presented above and its characteristics, it is important to bring even more clarity on the difference between blockchain and DLTs and their specific features. At the beginning of this report it has been mentioned that blockchain and DLT concepts are similar but not the same thing. This chapter will detail their main characteristics and compare them.

The confusion is mainly created because both, blockchain and DLTs, refer to a database or set of records that are distributed across a network and promote a higher level of transparency and openness comparing with the traditional centralized systems. However, despite these characteristics which seem to be relevant for the two concepts, they have features which differentiate them fundamentally.

3.1. Permissionless vs. Permissioned

The main difference between blockchain and DLT is determined by how open is the network in which they are deployed to the general public.

In the case of blockchain, the network is fully open meaning [40]:

- 1) Anyone can join the network and remain generally anonymous;
- 2) All participants can run a node and become part of the governance mechanism;
- 3) All participants can read or write data within the blockchain and participate in confirming transactions independently.

That is why blockchain is considered “permissionless”.

On the other side, DLTs is normally open to a limited number of players; hence, is less decentralized and restricts aspects, such as [40]:

- 1) Who can access the network (participants are well known),
- 2) Who can operate as a full node (authorization is needed to keep a copy of the ledger), and
- 3) Who can be a validator and have write access (permission is required to participate in consensus).

This is the reason why, DLTs are also known as “permissioned” networks.

3.2. Understanding the Differences

As presented in Table 3.1, there are few characteristics of blockchain and DLT that require more clarifications.

Table 3.1. Comparison between blockchain and DLT features [41]

	Blockchain	DLT
Governance	Decentralized	Mostly centralized
Access	Anonymous / Pseudonymous	Identified
Trust in centralization	Low	High
Control resistance	High	Low
Consensus	“Everybody” votes	Few vote
Token	With	Usually without
Performance	Low	High

On the one hand, in blockchain, governance is decentralized in relation to the participating nodes in the network which are all holding a copy of the ledger and how they reach the consensus. However, it has to be highlighted that over time the mining process has become less decentralized (for example in case of Bitcoin) due to the fact that simple individuals participating as miners in the blockchain do not have enough hashing power to mine blocks regularly. Thus, they join centralized blockchain pools that aggregate the mining power and share the profits. On the other hand, DLTs are mostly governed centrally by one or few nodes acting as validators and deciding which other nodes may have read access in the network. As a result, the power in the DLT network is not distributed equally between members.

Further, this difference, in terms of governance, implies that the blockchain’s trust in centralization is low while DLT relies on this type of trust. As a consequence, DLTs have low censorship resistance since it is not a relevant requirement of the network– normally DLTs are implemented as a consortium where all participants are identified, have trust and know each other. On the contrary, access to blockchain is done, in most of the cases, anonymously without the obligation to submit personal information in order to operate in the network. However, Bitcoin is pseudonymous meaning that even if the transactions are visible to the participants in the network, the identity of the users associated with the transactions is not, it is attached to their private keys [42], and might be inferred using heuristic algorithms. Identity confidentiality is very controversial because while it is desirable to comply with privacy legislation (e.g., GDPR), it can facilitate fraud and obstruct the use of transparency laws (e.g., Anti-Money Laundering (AML)) [27].

Another difference between blockchain and DLT relates to the mechanism used to validate the transactions. While blockchains are driven by consensus protocols and allow everybody to run a full node and confirm new blocks even if they do not belong to the mining pools or are the first to solve the puzzle, DLTs restrict the possibility to run nodes on the network, read, write or validate transactions and as a result there is no need for consensus of the entire network to agree on a change.

It is important to highlight as well that blockchain is based on the assumption that the participants on the network are potentially corrupt. In this sense, most blockchain implementations provide an incentive model where validators are rewarded through monetary or utility tokens (depending on the scope they serve) to motivate them to behave properly, create value, and ensure the integrity of the network. In addition, these incentives reward the computational cost of the miners who are able to resolve the cryptographic puzzle. On the other hand, DLTs relies on members who trust each other

and have bilateral contractual agreements between them. Hence, as a consequence, they do not need tokens as incentives to protect themselves against any malicious behaviour [43].

While tokenized incentives ensure security and integrity, they are impacting in a negative way the performance of the network. Blockchains are slow and can process a much lower number of transactions per second (TPS) comparing with DLTs or the traditional centralized solutions (such as Visa). This weakness makes blockchain unable to support the deployment of applications that requires high transaction volumes on large scale [43].

Considering all these aspects it is difficult to conclude if one architecture is better than the other, it is more appropriate to assume that each of them might represent a good solution for certain use cases while accepting that sometimes centralization might still be preferred to resolve particular problems.

4. Landscape and Characteristics

While the main groups that are part of the standardization landscape for blockchain and DLTs were described in the Chapter 2, this chapter clarifies more in detail the work done by selected groups, ISO and ITU.

4.1. International Organization for Standardization (ISO)

As mentioned previously, the first ISO standard, which was released in September, 2019 under ISO/TR 23455: 2019 based on the work done within WG3, presents the history of smart contracts and how they are implemented using an underlying distributed ledger [14].

While distributed ledgers, including blockchains, allow a fair distribution of decision-making power among stakeholders who may have different interests in agreeing to change the content of a ledger they share, smart contracts take this concept one step further. They are computer programs that are stored in a distributed ledger, and that rely on such repository to ensure the automatic enforcement of contractual obligations between the participants. The reason why these contracts are called “smart” is because they perform autonomously being installed and executed at selected peers. In addition, the proper execution of the smart contracts has to be authorized by all or the majority of the validators in order for the output of such a smart contract to be written in blockchain.

The technical report describes the fundamental concepts of smart contracts. It starts with a short history of the concept of smart contracts which was introduced for the first time by Nick Szabo in 1997. It continues by presenting them from three different perspectives [15]:

- As a **“piece of code”** meaning that they automate the contractual conditions and what is exchanged with the contract,
- As a **“code as law”** where the code behind smart contracts operates as a law unto itself, and
- As defined by legal professionals and enforced by conventional law.

Moreover, the report details the life cycle and operation, transfer from one distributed registry to another, legal considerations but provides as well examples of smart contract implementations. In addition, the report explains the functions of smart contracts and how they interact with each other on blockchains and distributed ledger environments. It is also the starting point for other standards

currently being developed by ISO technical committee ISO/TC 307, and more specifically by its working group WG3 *"Smart Contracts"*.

The WG2 released in May 2020, a standard related to *"Privacy and personally identifiable information protection considerations"* under ISO/TR 23244. Currently, there is not a lot of data available free of charge about its content but from the information made public it proposes a privacy framework for blockchain and DLT systems by identifying what can be considered Personally Identifiable Information (PII) and what are the legal, regulatory and business requirements for privacy. From the very beginning is being highlighted that this standard adheres to the privacy principles of ISO/IEC 29100:2011/Amd 1:2018, Clause 5 which are referring to use, retention and disclosure limitation, accuracy and quality, openness, transparency and notice, information security, privacy compliance of PII and much more. In addition, it assesses the privacy impact on blockchain and DLTs as part of overall risk management program and how it has to be managed from change management, monitoring, review and continuous improvement as well as compliance point of view [16][17].

Another standard that is currently under preparation for its final publications is ISO/DIS 22739(en) *"Blockchain and distributed ledger technologies - Terminology"*. As of today, there are many definitions available for the basic terms used in relation to blockchain and DLTs and in many cases there is no common understanding of those concepts in practice. That is why the main scope of this standard is to define a similar language and unified vocabulary related to blockchain and DLTs to be used across the other documents issued within the scope of ISO/TC standards but also in this industry. In its draft version, the document provides definitions for 84 concepts, out of which 12 were taken over from the existing ISO definitions [18].

The rest of seven ISO standards in the scope of TC 307 are still in development in early stages. That is why it is not possible to provide further aspects of the efforts that are currently made within ISO to standardize the blockchain and distributed ledger industry.

4.2. The International Telecommunication Union (ITU)

At ITU level, the first recommendation issued by the first working group had as scope to identify and describe the most commonly used terms in the context of distributed ledger technology. In case of some terms, a figure has been added to provide additional clarity. As part of this report, 62 terms are being defined, out of that 20 concepts are taken over from ISO or other organizations that already initiated work in this direction [21].

The second technical report delivered by the first working group targeted to provide transparency with regard to overview, concept and ecosystem for the distributed ledger technology. It starts by explaining the key features of DLT systems which are immutability, sharedness, distribution and append only database. It continues with the classification of DLTs into permissionless, permissioned and hybrid and with a detailed description of three consensus mechanisms: Proof of Work (PoW), Proof of Stake (PoS) and Byzantine fault tolerant-based. Finally, a large space has been allocated to the ecosystem and its aspects: hardware, business, software and protocol development [22].

The last report of the first working groups provides an up to date overview of the DLT standardization landscape. It lists the ITU work in progress of its study groups in the context of DLTs about security, e-services, cloud computing and trusted network infrastructures or Internet of things (IoT) as well as its initiatives that are already completed: FG DLT which is already detailed above, digital currency, data processing and management to support IoT and smart cities, digital financial services or environmental efficiency for artificial intelligence or other emerging technologies. In addition, the

report enumerates the efforts done within the same scope by other international (ISO, IEEE, W3C, etc.) or local organizations (DIN, UNE) or even community or industry groups (Linux Foundation, Ethereum or BiTA) [23].

The DLT use cases technical report is one of the most valuable deliverables of FG DLT and it was in the scope of work group two (WG2). It highlights the advantages as well as the challenges related to the implementation and use of DLTs and emphasizes how the Sustainable Development Goals (SDGs) can be achieved by using this innovation (see Table 3 from Appendix B for details). It also consolidates several real-world use cases and explains how those could profit from the standardization effort. The uses cases are assigned to vertical and horizontal domains. Vertical domains refer to the sectors where DLTs can be implemented such as finance, healthcare, information and communication technology (ICT), industry while the horizontal domain includes the types of services that are applicable to the verticals, e.g., identity management, security or data management [24].

Another report of high importance was issued by the work group three (WG3) and details the technical specification of the DLT's architecture and its core functions and components. This document has been created by mapping the architecture of fourteen live DLT platforms (see Figure 4.1.).

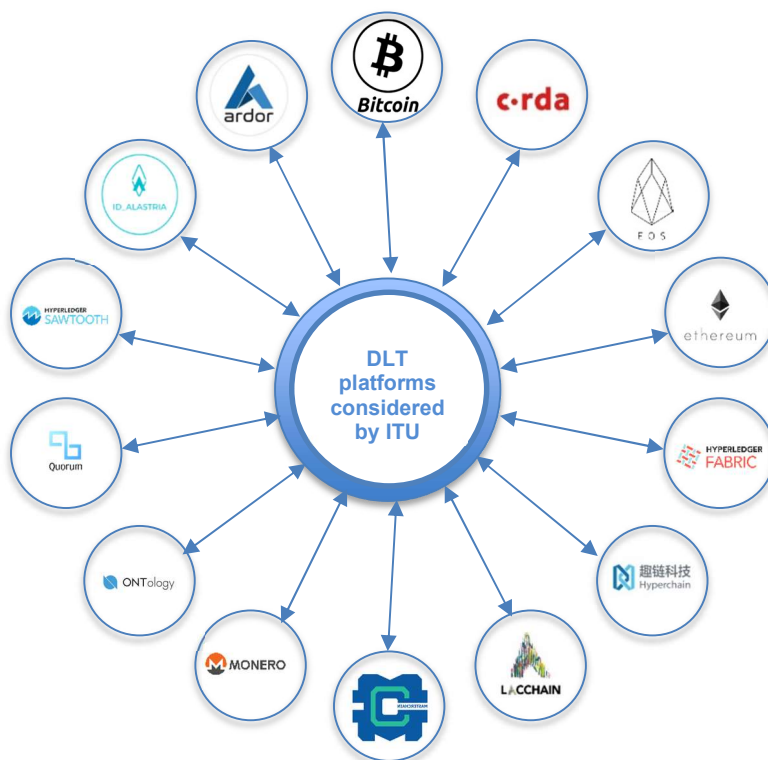


Figure 4.1. Overview of ITU architecture mapping to existing DLT platforms [25]

Another technical specification released by WG3 lists the assessment criteria for selecting a DLT platform. Decision making process should consider standards related to DLT core functions, as well as criteria for DLT application functions or operation functions (see Figure 4.2. for details).

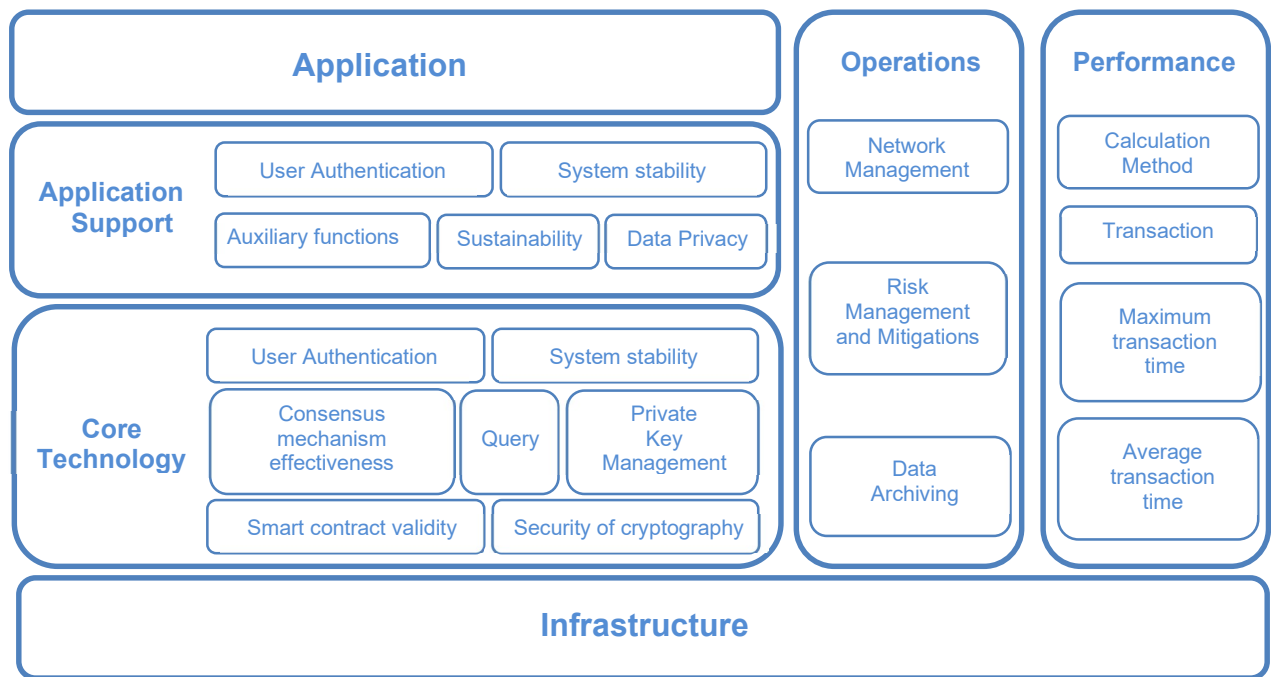


Figure 4.2. Overview of DLT assessment framework [26]

Last but not least, performance or the related ecosystem (platform maturity, maintenance, running cost, availability of professionals, etc.) are also essential in the selection process [26].

The work group four (WG4) took the responsibility of issuing a report about regulatory framework. This document proposes practical advice to users, regulators or technologists about how to mitigate related DLT possible risks. Five DLT associated features and their regulatory challenges are being in focus:

- Distribution and ledger sharing,
- Autonomy and responsibility,
- Temper evidence and resistance,
- Incentive mechanism and digital assets,
- Openness, transparency and anonymity.

The report concludes that global legislation and regulations has to be adapted to consider both opportunities and risks associated to DTLs and highlights that there are areas (e.g., blockchain immutability) which are in conflict with the existing laws and an immediate solution for such problems requires a partnership between regulators and organizations involved in this industry [27].

The last technical report issued by ITU in work group five (WG5) is an outlook on distributed ledger technologies. It tries to identify the latest trends related to DLT in order to anticipate the future of this innovation. The DLT evolution is analysed based on several dimensions [28]:

- Government and Regulation,
- Computation networks,
- Identity and Privacy,
- Security and Resilience,
- Risk and Audit.

5. Discussion on the Consensus

“The importance of developing effective governance frameworks through standards and other publications will ensure the confidence of future users of this technology.” [...] “Developing and setting standards requires consensus, which encourages an international community of experts to share, collaborate and agree.” Daniel Chidgey, Head of Stakeholder Engagement from Standards Australia [44]. This sentence is a good sum-up to precede with the discussion about consensus between the groups described in Chapter 4 which are currently driving the standardization initiative.

5.1. Agreeing on Terminology

One essential factor for the standardization of blockchain and DLT is the employment of equal definitions of related terms by different organizations. This factor was a priority for both ISO and ITU in beginning of their efforts.

ITU dedicated its first technical specification on defining the vocabulary used in the context of blockchain and DLT [21]. In total, 62 terms were explained in the report and separate notes and figures supported additional clarifications on such terms. In contrast, ISO has not released yet the document related to terminology. However, it is now under preparation for its final publication. ISO has defined in this standard 84 terms and for many of them has used complementary notes to offer more clarity [18].

As presented in Appendix C, Table 1 only 28 terms are commonly defined, out of which 11 share exactly the same definitions which have been taken from ISO/TC 307. However, the rest of the 17 jointly described terms which are very similar and consistent in their definitions.

Important to remark is that the majority of terms are still specific to either ISO or ITU vocabulary. One reason for this difference might be related to the work scope of the two groups. While ITU is ICTs, ISO scope is more broadly across all the industries. This means that, in case of ISO, some of the terms which are not necessarily specific to blockchain or DLT (such as account, address, compliance, etc.) are already defined as part of other issued standards and are not included in the scope of ISO/TC 307 standards. Another observation is that some of the terms are being explained in the context of blockchain and DLT by associating them with other terms (such as block data, crypto-asset, reward system, etc). Last but not least, some of the definitions refer to the same thing even if the terms are not always identical. For example, fault tolerance defined in ISO means the same as Byzantine fault tolerance defined in ITU, or cryptographic hash function in ISO and hash function in ITU.

5.2. Smart Contracts

ISO released in 2019 its first standard for blockchain and DLT and dedicated it to the “*Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*” [14]. Actually, within ISO/TC 307, WG3 focuses its efforts completely on smart contracts and their applications. On the other hand, the approach of ISU is a little bit different. This topic is being addressed by most of its focus groups depending of their specific work.

However, independent of the methodology used, both standardization groups analyse smart contracts in relation to their legal effects and the conflict they may generate between the public-law

order and privacy rights. One proposed way to solve this problem is to avoid keeping personal data on the blockchain and use sidechains or other private storage for PII and sensitive data. Crosschain techniques need to be developed to facilitate transactions across sidechains. In the same context the terms of on-chain/off-chain of smart contracts are being introduced as practices to solve disputes with laws and reduce the computational compensation. The recommendation in this case is as well to store the private information of the smart contract off-chain, while deploying the remaining part on-chain. This way, the sensitive information can be hidden from the public and on the same time the mining cost can be reduced [14][15][27].

“In the future, blockchain enabled smart contracts will sit hidden inside the engines of online systems reducing or even eliminating certain types of fraud, mistake and leakage, that until now we have all had to live with,” said Philippa Ryan, Chair of the Australian Subcommittee for Smart Contracts. [44]

In this sense, special attention is being given to the security verification of smart contracts and how they are programmed. Ultimately, they represent a piece of software stored on the ledger; hence, they might contain bugs or need to be updated and upgraded. Currently, new programming languages are developed to target blockchain and DLTs, make smart contracts more secure, easier to be deployed and tested. In such a context, standards are needed to harmonize the way how source code of smart contracts is being understood and how these can be developed [14][28].

Last but not least, both ISO and ITU dedicated space in their reports to present examples of smart contract implementations as well as use cases. For example, ITU mapped the DLT architecture to 14 existing platforms (see Figure 4.1) and highlighted if and how they use smart contracts [25]. In addition, it shortly presented their use cases from finance, arts, eSports, public sector, and international relations [24]. ISO focused as well on how different players in the blockchain and DLT space (e.g., Corda, Ethereum, and Hyperledger Fabric) implemented smart contracts and reviewed a few applications and smart contract use cases.

5.3. Privacy and PII for Blockchain/DLT Systems

Privacy and PII's protection is a broader topic that is not only linked to the smart contracts but its related issues are considered a major concern for the adoption on large scale of the blockchain and DLTs. This barrier has been recognized by both, ISO and ITU, which put considerable efforts into analysing the subject and providing guidance.

ISO had already standards for privacy and the processing of PII (such as ISO/IEC 29100, *“Information technology - Security technique - Privacy framework”* and ISO/IEC 29134:2017 *“Information technology - Security techniques - Guidelines for privacy impact”*) and these were considered as basis for the new standard (ISO/TR 23244 *“Blockchain and distributed ledger technologies - Privacy and personally identifiable information protection considerations”*) issued in May 2020 in the context of blockchain and DLTs [16][17].

ISO and ITU evaluate the privacy in relation to the legal and regulatory requirements. Few concerns are being emphasized [17][28]:

- Participants involved in blockchain and DLT may be located in different countries with different legal and regulatory environments; hence, it is not always easy to ensure legal certainty under a recognized legal jurisdiction. In addition, in some cases the legal requirements might be even conflicting.
- Blockchain and DLT as decentralized systems do not have a specific “owner” and as a consequence there is no clearly defined legal status for applying the accountability principle as required by ISO/IEC 29100:2011/Amd 1:201.

- Due to immutability, transactions in blockchain and DLT cannot be modified or deleted and this could be in conflict with GDPR for example, and represents a high risk for persons or organizations that must comply with these rules.

In addition, ITU is highlighting that there is a common interest of some countries, such as France and its data protection authority CNIL, or the Austrian *Datenschutzbehörde*, and even on European Union (EU) level through its Blockchain Observatory to address these limitations and make recommendation on how to solve these problems. However, at the moment, there are still legal uncertainties. Meanwhile, according ITU, there are three best practices used to ensure the privacy and protection of PII [28]:

- Storing of private information off-chain and limit the access to such information to only authorized parties [28].
- Using sidechains as parallel systems to keep especially sensitive data such as PII. A sidechain can even be removed without losing the integrity of the parent system and this way it can comply with right-to-be-forgotten obligation of GDPR.
- Applying Zero-Knowledge Proof (ZKP) as a cryptographic technique to prove that a transaction is true without publishing the information about the participants to the transaction or its details. It relies only on the two parties involved.

Finally, there are additional recommendations proposed by ITU when it comes to personal or sensitive data which must be taken into consideration:

- Perform privacy and data impact analysis and assess the identified risks.
- Encryption of personal data has to be very strong to avoid that hashed data can be easily guessed.
- Prevent relying entirely on consensus for private and sensitive data.

6. Conclusions

This report presented the main international or local standardization activities in the blockchain and DLTs space while drawing attention to potential misunderstandings related to these concepts or their architecture and emphasising how crucial is to reach consensus to support this industry to emerge. Thus, it clarified misconceptions regarding the differences between blockchains and DLTs, providing a common ground for the understanding of the standardization activities.

Based on the described standardization efforts, it becomes clear that simplifying and harmonizing the procedures related to how to operate and deploy a blockchain or a DLT through standards is key for allowing potential participants to join these networks and to provide solid applications taking advantages of the benefits provided by these two novel technologies.

“Trusted standards mean that industry doesn’t need to reinvent the wheel, that innovations will be compatible and work with existing technology, and that products and services will be trusted, too. Governments use standards as trusted solutions to complement regulation, and they give peace of mind to consumers who know they are not putting themselves or their families at risk.” - Acting ISO Secretary-General Kevin McKinley [45]. With such a quote in mind, it can be concluded that blockchain and DLTs standardization will provide globally approved methods to operate and accelerate acceptance as well as better interoperability with other technologies or between existing networks with the ultimate goal to innovate how they are applicable or used.

APPENDIX A - ISO WORK STRUCTURE

Table 1 - Participating, observing members and liaison organizations (as of June, 2020)

Participant countries	Acronym	Observing countries	Acronym	Liaison Organizations	Title
Australia	SA	Argentina	IRAM	EC	European Commission
Austria	ASI	Belarus	BELST	EEA Inc.	Enterprise Ethereum Alliance Inc.
Belgium	NBN	Colombia	ICONTEC	FIG	International Federation of Surveyors
Brazil	ABNT	Estonia	EVS	GS1	GS1
Cambodia	ISC	Hong Kong	ITCHKSAR	IEEE	Institute of Electrical and Electronics Engineers, Inc
Canada	SCC	Indonesia	BSN	INATBA	International Association for Trusted Blockchain Applications
China	SAC	Iran, Islamic Republic of	ISIRI	ITU	International Telecommunication Union
Croatia	HZN	Kenya	KEBS	OECD	Organization for Economic Co-operation and Development, OECD
Cyprus	CYS	Morocco	IMANOR	SBS - Small Business Standards	Small Business Standards
Czech Republic	UNMZ	Philippines	BPS	SWIFT	Society for Worldwide Interbank Financial Telecommunication
Denmark	DS	Romania	ASRO	UNECE	United Nations Economic Commission for Europe
Finland	SFS	Slovakia	UNMS SR		
France	AFNOR	Uruguay	UNIT		
Germany	DIN				
Hungary	MSZT				
India	BIS				
Ireland	NSAI				
Israel	SII				
Italy	UNI				
Jamaica	BSJ				
Japan	JISC				
Kazakhstan	KAZMEMST				
Korea, Republic of	KATS				
Luxembourg	ILNAS				
Malaysia	DSM				
Malta	MCCAA				
Mexico	DGN				
Netherlands	NEN				
New Zealand	NZSO				
Nigeria	SON				
Norway	SN				
Poland	PKN				
Portugal	IPQ				
Russian Federation	GOST R				
Singapore	SSC				
South Africa	SABS				
Spain	UNE				
Sweden	SIS				
Switzerland	SNV				
Thailand	TISI				
Ukraine	DSTU				
United Arab Emirates	ESMA				
United Kingdom	BSI				
United States	ANSI				

Source: <https://www.iso.org/committee/6266604.html> [10]

Table 2 - Standard and/or project under the direct responsibility of ISO/TC 307 Secretariat

Title	Stage	ICS	Status
ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems	60.60	35.030 35.240.40 35.240.99	Published
ISO/TR 23244: 2020 Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations	60.60	35.030 35.240.40 35.240.99	Published
WG1: Foundations			
ISO/FDIS 22739 Blockchain and distributed ledger technologies — Vocabulary	50.20	35.030 01.040.35 35.240.40 35.240.99	Proof sent to secretariat or FDIS ballot initiated: 8 weeks
ISO/CD 23257.3 Blockchain and distributed ledger technologies — Reference architecture	30.60	35.030 35.240.40 35.240.99	Close of voting / comment period
ISO/WD TS 23258 Blockchain and distributed ledger technologies — Taxonomy and Ontology	20.20		Working draft (WD) study initiated
WG2: Security, privacy and identity			
ISO/CD TR 23576 Blockchain and distributed ledger technologies — Security management of digital asset custodians	30.60	35.030 35.240.40 35.240.99	Close of voting / comment period
ISO/CD TR 23245.2 Blockchain and distributed ledger technologies — Security risks, threats and vulnerabilities	30.20	35.030 35.240.40 35.240.99	CD study / ballot initiated
ISO/CD TR 3242 Blockchain and distributed ledger technologies – Use cases	30.00		Committee draft (CD) registered
WG3: Smart contracts and their applications			
ISO/AWI TS 23259 Blockchain and distributed ledger technologies — Legally binding smart contracts	20.00		New project registered in TC/SC work programme
JWG4: Joint ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG; Blockchain and distributed ledger technologies and IT Security techniques			
ISO/NP TR 23246 Overview of identity management using blockchain and distributed ledger technologies*			Cancelled
WG5: Governance			
ISO/AWI TS 23635 Blockchain and distributed ledger technologies — Guidelines for governance	10.99		New project approved
WG6: Use cases**			
ISO/CD TR 3242 Blockchain and distributed ledger technologies – Use cases	30.00		Committee draft (CD) registered
SG7: Interoperability of blockchain and distributed ledger technology systems			
ISO NP TS Interoperability Framework			For NWIP ballot

* The Technical Report of JWG4: ISO/NP TR 23246 "Overview of identity management using Blockchain and DLT" did not reflect recent advancements in the area of Identity well. This technical report has been cancelled and, instead, a completely new Technical Report on "Overview of existing DLT systems for identity management" is planned.

** In the frame of WG6 "Use cases" the EC proposed EBSI "Identity" use case, which has been confirmed by the working group as eligible to be included in the upcoming publication. Additionally, in the future iterations it could be expected that one more use case EBSI "Diploma" will be included as well. It is particularly interesting as an example of possible interoperability with a similar use case proposed by India.

Source: <https://www.iso.org/committee/6266604/x/catalogue/> [11]

APPENDIX B - ITU WORK STRUCTURE

Table 1 – Detailed summary of FG DLT Meetings

Meeting	Host	Inputs	Outputs	Meeting report	Remote participants	Total participants	Co-located events
Geneva, 17-19 October 2017	ITU	39	7	O-007	24	81	-
Bern, 5-7 February 2018	Swisscom	37	12	O-019	23	64	-
Geneva, 28-30 May 2018	ITU	26	12	O-028	29	60	-
Beijing, 9-12 October 2018	CAICT, Trusted Blockchain Initiatives	21	14	O-045	16	47	Trusted Blockchain Summit 2018
Rio de Janeiro, 14-17 January 2019	BNDES	34	12	O-057	31	67	Workshop on DLT for transparency and integrity
Madrid, 1-4 April 2019	Alastria	41	13	O-070	20	48	Workshop on DLT, Blockchain and SDG Attainment
Geneva, 29 July - 1 August 2019	ITU	24	12	O-082	15	62	Workshop on DLT scalability and interoperability
Total		223	82		158	429	

Source: <https://www.itu.int/md/T17-TSAG-190923-TD-GEN-0475> [19]

Table 2 - Summary of FG DLT deliverables

Number	Type	Title	Text	Description
D1.1	Technical Specification	DLT terms and definitions	PDF DOCX	This document contains a baseline set of definitions of terms commonly used in DLT. The definitions provide a basic characterization of the term, and where appropriate, a note is included to provide additional clarity.
D1.2	Technical Report	DLT overview, concepts, ecosystem	PDF DOCX	This document provides an overview, concept and ecosystem for the distributed ledger technology.
D1.3	Technical Report	DLT standardization landscape	PDF DOCX	This document describes the standardization landscape for DLT, as of July 2019. It covers ITU-T, ISO, IEEE Standards Association, W3C, UNECE/CEFACT, ETSI, CEN/CENELEC, NIST, DIN, and other communities.
D2.1	Technical Report	DLT use cases	PDF DOCX (Report only) ZIP (Report and use cases)	This document consolidates each of the real-world use cases gathered during the lifetime of the ITU-T FG DLT. It also consolidates the knowledge extracted from these use cases, highlighting the competitive advantage of each use case brought by DLT, the main barriers to DLT adoption, how new business models based on DLT can contribute to the attainment of the SDGs and how the use cases could benefit from a standardization effort.
D3.1	Technical Specification	DLT reference architecture	PDF DOCX (Specification only) ZIP (Specification and platform mapping)	This document defines the reference architecture for distributed ledger technology, the hierarchical relationship and specific functions of the distributed ledger technology architecture, important modules and specific functions in the structure of distributed ledger technology, the main technical route and direction of the core module in the distributed ledger architecture. The mapping of this DLT reference architecture to popular DLT platforms was conducted and the results contained in the attachments to this report.
D3.3	Technical Specification	Assessment criteria for DLT platforms	PDF DOCX	This document defines an assessment framework for a DLT platform, which includes a set of criteria for function, performance and other aspects. The framework can be used as a guideline for DLT platform assessment as well as information disclosure of a certain DLT platform product.
D4.1	Technical Report	Distributed ledger technology regulatory framework	PDF DOCX	This document considers the key properties of DLT that are common among the diversity of many approaches. We aim to bring into focus the topics that are of concern to the regulators. By supplying practical recommendations for users, regulators, and technologists, we hope to mitigate the risks of potential harms.
D5.1	Technical Report	Outlook on distributed ledger technologies	PDF DOCX	This document explores the advancement of DLT beyond legacy landscapes, frameworks, architectures and introduces the emerging concepts related to DLT.

Source: <https://www.itu.int/md/T17-TSAG-190923-TD-GEN-0475> [19]

Table 3: DLT Solutions for Key Challenges in Sustainable Development Goals (SGDs)

SGD #	Challenge	Solution (one example)
1	One in ten people in Low-Middle-Income Countries (LMCs) are living with their families on less than the international poverty line of US\$1.90 per day.	DLT can automatically record transactions on a secure ledger with near-instantaneous financial settlement. This means there are shorter payment cycles in comparison to traditional banking and third-party payment methods. Such efficiencies could be harnessed to help address poverty, as they promote more transparent and equitable trade, which, in turn, helps to ensure that all men and women –particularly the poor and vulnerable –have equal rights to economic resources.
2	Not all people (and especially children) have access to sufficient and nutritious food all year round.	DLT could strengthen the supply side, particularly for small-scale food producers and family farmers, thus enabling them to better access markets and receive equal treatment in the supply chain.
3	Non-communicable diseases and mental health have been attracting new attention and funding; competing with the traditional focus on infectious diseases such as HIV, TB and Malaria.	DLT can support enhanced prevention and treatment outcomes through, for example, breaking down data silos across medical providers and enabling the tokenization and incentivization of physically or mentally beneficial activities.
4	Access to inclusive education	DLT-based platforms could connect students, educators, and service providers where, together, they develop and engage in personal and group online sessions, as well as in-person educational programs where progress, attendance, and completion are automatically tracked.
5	Discrimination against women and girls globally	DLT could help women earn and retain control over additional income. DLT also has the potential to mitigate on-line harassment.
6	Clean water is an essential resource for life, yet its distribution is globally unbalanced.	DLT combined with IoT sensors enables households, industries, water managers, and policymakers to all access the same data on water quality and quantity in order to make more informed decisions.
7	Increasing the share of renewable energy and doubling the efficiency of energy production.	DLT enables the ability to tokenize energy trading platforms, allowing consumers to trade the energy from solar panels and batteries in a peer-to-peer network, incentivizing the introduction of new devices to local microgrids
8	1) Government access to domestic financing at a reasonable cost and 2) Access to interest bearing savings instruments for the poor and emerging middle class with an emphasis on the emerging middle class because the really poor have no money to invest at all.	DLT can allow the sale of small value mobile retail bonds and promote inclusive growth in an economy by democratizing sovereign debt.
9	Economic development	Trading with a DLT-based regulatory-compliant global currency can enable micro-transactions which are an important enabler of services and particularly services tailored for the poor.
10	Reducing inequalities in the economy, governance, rights and decision making.	DLT can enable better economic equality by reducing the costs of remittances. It can also open new avenues for citizens to get involved in decision-making through secure voting initiatives.
11	Two thirds of the world's population will be living in cities by 2050 (2.5 billion more than today) and by 2030 the world is expected to have 43 megacities with more than 10 million inhabitants compared with 31 today	DLT can provide a cost effective and trustworthy enhancement for local democracy within cities, allowing neighbourhoods and large housing developments, to have a voice, through voting, on decisions that affect them.
12	Transparency and visibility of value chain and production processes are key steps for gaining a better understanding of social, environmental and health risks and ensuring due diligence.	Tracing of products in supply chains relates closely to consumers awareness of the origins of products, sustainable production methods, and health implications.

13	Challenges to the ability of the world to meet climate change goals, creating the risk of irreversible ecological disaster	DLT can be implemented to support the development of carbon marketplaces. While traditional technologies are subject to accounting flaws and fraud –which have held back the development of such marketplaces in the past, DLT platforms for trading assets which represent carbon could guarantee immutability and transparency.
14	Protect marine and coastal ecosystems from pollution, as well as address the impacts of ocean acidification and other negative practices such as over-fishing.	DLT can combat overfishing and wildlife trafficking by providing the baseline architecture for interoperable data collection, allowing better management of ecosystems, more informed decision making across organizations, and increased accountability around catch types and quantities since competing organizations must share the same ledger.
15	Reversing the effects of land degradation and desertification through sustainable land management	DLT can be used to incentivize organizations and individuals to increase the scale and efficiency of conservation protection by offering small cash payments in exchange for conserving nature.
16	Strengthening the rule of law is the fundamental key for success in this process of achieving peace.	Smart contracts executed on DLT platforms can be used to automate and enforce agreements between business entities.
17	Coordinating policies to help developing countries manage their debt, as well as promoting investment for the least developed, is vital to achieving sustainable growth and development	DLT can be used to facilitate partnerships and collaboration between governments, companies, academia, civil society and individuals where trustworthy information and value transfers are needed. Bridging the digital divide and increasing digital literacy with enhanced use of DLT can support the empowerment and capacity building of communities and regions on both the domestic and international level.

Source: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf> [24]

APPENDIX C - ISO AND ITU CONSENSUS

Table 1 – Comparison of common definitions provided by ISO and ITU

	ISO	ITU	Source
asset	anything that has value to a stakeholder	representation of value.	
block	data structure comprising a block header and block data	individual data unit of a blockchain, composed of a collection of transactions and a block header. NOTE –A block may be immutable and considered as the digital entity, however, it can be applied to other networks or other computational facilities.	
block header	data structure that includes a cryptographic link to the previous block Note 1 to entry: A block header can also contain a timestamp, a nonce, and other DLT platform specific data, including a hash value of corresponding transaction records.	data structure that includes a cryptographic link to the previous block.	[b-ISO/TC 307]
blockchain	distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links Note 1 to entry: blockchains are designed to be tamper resistant and to create final, definitive and immutable ledger records.	a type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision	
consensus	agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions Note 1 to entry: Consensus does not necessarily mean that all DLT nodes agree. Note 2 to entry: The details regarding consensus differ between blockchain designs and this is one key distinguishing characteristic between one design and another.	agreement that a set of transactions is valid.	
consensus mechanism	rules and procedures by which consensus is reached	rules and procedures by which consensus is reached	
decentralized system	distributed system wherein control is distributed among the persons or organizations participating in the operation of system. Note 1 to entry: In a decentralized system, the distribution of control among persons or organizations participating in the system is determined by the system's design.	distributed system wherein control is distributed among the persons or organizations participating in the operation of system.	[b-ISO/TC 307]
fork ledger split	creation of two or more different versions of a distributed ledger originating from a common starting point with a single history	creation of two or more different versions of a distributed ledger. NOTE –There are two types of forks: hard fork and soft fork.	
genesis block	first block in a blockchain Note 1 to entry: A genesis block has no previous block and serves to initialize the blockchain.	The first block in a blockchain that serves to initialize the blockchain.	

hard fork	change to a DLT platform in which new ledger records or blocks created by the DLT nodes using the new version of the DLT platform are not accepted as valid by DLT nodes using old versions of the DLT platform Note 1 to entry: If not adopted by all DLT nodes, a hard fork can result in a ledger split.	change to the protocol or rules that result in a fork that is not backward compatible	
ledger	information store that keeps records of transactions that are intended to be final, definitive and immutable	information store that keeps final and definitive (immutable) records of transactions.	
Merkle tree	tree data structure in which every leaf node is labelled with the hash value of a data element and every non-leaf node is labelled with the hash value of the labels of its child nodes	a data structure where the data is hashed and combined until there is a singular root hash that represents the entire data structure.	
node	<data structure> elementary component from which a data structure is built	device or process that participates in a distributed ledger network. NOTE –Nodes can store a complete or partial replica of the distributed ledger.	
off-chain	related to a blockchain system, but located, performed or run outside that blockchain system	related to a blockchain system, but located, performed or run outside that blockchain system.	[b-ISO/TC 307]
on-chain	located, performed or run inside a blockchain system	located, performed or run inside a blockchain system	[b-ISO/TC 307]
peer-to-peer	relating to, using, or being a network of peers that directly share information and resources with each other without relying on a central entity.	relating to, using, or being a network of equal peers that share information and resources with each other directly without relying on a central entity	[b-ISO/TC 307]
permissioned	requiring authorization to perform a particular activity or activities Note 1 to entry: The usual interpretation of “permissioned” implies the need for an identity for the entity involved, to which authorization is granted. It is typical for there to be both organization identities and also identities for individuals (e.g. DLT users)	requiring authorization to perform a particular activity or activities	[b-ISO/TC 307]
permissioned distributed ledger system	distributed ledger system in which permissions are required	distributed ledger system in which permissions are required to maintain and operate a node.	
permissionless	not requiring authorization to perform any particular activity	not requiring authorization to perform any particular activity	[b-ISO/TC 307]
permissionless distributed ledger technology system permissionless DLT system	distributed ledger system that is permissionless	distributed ledger system in which permissions are not required to maintain and operate a node. NOTE –Examples of permissionless ledger are the Bitcoin and Ethereum blockchains, where any user can join the network and start mining	
private distributed ledger technology system private DLT system	distributed ledger system which is accessible for use only to a limited group of DLT users Note 1 to entry: public and private categories apply to the users of a distributed ledger system, and permissioned or permissionless categories apply without distinction between users and operators	distributed ledger system which is accessible for use only to a limited group of DLT users	

public distributed ledger technology system public DLT system	distributed ledger system which is accessible to the public for use	distributed ledger system which is accessible to the public for use	[b-ISO/TC 307]
smart contract	computer program stored in a distributed ledger system wherein the outcome of any execution of the program is recorded on the distributed ledger Note 1 to entry: A smart contract might represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction.	program written on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions.	
Soft fork	change to a DLT platform in which some records or blocks created by the DLT nodes using the old version of the DLT platform are not accepted as valid by DLT nodes using new versions of the DLT platform Note 1 to entry: a soft fork can result in a ledger split	change to the protocol or rules that result in a fork that is backward compatible.	
subchain	logically separate chain that can form part of a blockchain system Note 1 to entry: A subchain allows for data isolation and confidentiality.	logically separate chain that can form part of a blockchain system	[b-ISO/TC 307]
token	digital asset that represents a collection of entitlements	a digital representation of value on a shared distributed ledger that is owned and secured using cryptography to ensure its authenticity and prevent modification or tampering without the owner's consent.	
transaction	smallest unit of a work process, which is one or more sequences of actions required to produce an outcome that complies with governing rules Note 1 to entry: where appropriate, transaction is understood more narrowly, as the smallest unit of a work process related to interactions with blockchain or distributed ledgers.	whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier	
wallet	application used to generate, manage, store or use private and public keys Note 1 to entry: A wallet can be implemented as a software or hardware module.	software and/or hardware used to generate, manage and store both private and public keys and addresses, which enable DLT users to transact. Some wallets may interact with smart contracts and allow single and/or multi-signature.	

Source: <https://www.iso.org/obp/ui#iso:std:iso:22739:dis:ed-1:v1:en> [18]

<https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf> [21]

References

- [1] Haber, S., Stornetta, W.S. *How to time-stamp a digital document*. J. Cryptology 3, 99–111 (1991). [Online]. Available: <https://doi.org/10.1007/BF00196791>
- [2] Institute of Chartered Accountants in England and Wales (ICAEW), *History of blockchain*. [Online]. Available: <https://www.icaew.com/technical/technology/blockchain/blockchain-articles/what-is-blockchain/history>
- [3] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2009. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [4] Nitish Singh, *Beginner's Guide: What is Distributed Ledger?* 2018. [Online]. Available: <https://101blockchains.com/what-is-distributed-ledger/>
- [5] Hasib Anwar, *Blockchain vs. Distributed Ledger Technology*. 2019. [Online]. Available: <https://101blockchains.com/blockchain-vs-distributed-ledger-technology/>
- [6] Oliver Belin, *The Difference Between Blockchain & Distributed Ledger Technology*. [Online]. Available: <https://tradeix.com/distributed-ledger-technology/>
- [7] Antik Patel, *History of the Blockchain*. 1991. [Online]. Available: https://medium.com/@ankit_233/history-of-the-blockchain-1991-38d6d4c3420c
- [8] Online Blockchain Event from 30 April 2020: *Use Cases, Tech Developments & Legal Perspectives*, organized by IBM Blockchain Switzerland
- [9] Benoit Abeloos, Gilbert Verdian, *Blockchain/DLT standardization workshop – Strategic Plan* [Online]. Available: https://ec.europa.eu/newsroom/document.cfm?doc_id=47026&usq=AOvVaw30PbLcdgSWKpUaCZAu2--x
- [10] *ISO/TC 307 Blockchain and distributed ledger technologies*. [Online]. Available: <https://www.iso.org/committee/6266604.html>
- [11] *Standards by ISO/TC 307 Blockchain and distributed ledger technologies*. [Online]. Available: <https://www.iso.org/committee/6266604/x/catalogue/>
- [12] *Overview of ISO/TC 307 plenary meetings*. [Online]. Available: <https://www.absolutassets.ch/single-post/2019/06/07/V-Plenary-of-ISO-TC-307-held-at-Dublin>
- [13] *Schedule of next planned ISO/TC 307 plenary meetings*. [Online]. Available: <https://www.iso.org/meeting-calendar.html>
- [14] *ISO/TR 23455:2019(en) Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems*. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso:tr:23455:ed-1:v1:en>

- [15] ISO 2019 *Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems* (extract). [Online]. Available: <https://cdn.standards.iteh.ai/samples/75624/ce1241c6670a4f65b1a6b93e1e5fce29/ISO-TR-23455-2019.pdf>
- [16] ISO/TR 23244:2020(en) *Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations*. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:75061:en>
- [17] ISO/TR 23244:2020(en) *Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations* (extract). [Online]. Available: <https://cdn.standards.iteh.ai/samples/75061/d664fb6259174565a6701cc50392251f/ISO-TR-23244-2020.pdf>
- [18] ISO/DIS 22739(en) *Blockchain and distributed ledger technologies — Terminology*. [Online]. Available: <https://www.iso.org/obp/ui/#iso:std:iso:22739:dis:ed-1:v1:en>
- [19] *Final report of FG DLT to TSAG*. [Online]. Available: <https://www.itu.int/md/T17-TSAG-190923-TD-GEN-0475>
- [20] *Focus Group on Application of Distributed Ledger Technology*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx>
- [21] *Technical Specification FG DLT D1.1 Distributed ledger technology terms and definitions*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d11.pdf>
- [22] *Technical Report FG DLT D1.2 Distributed ledger technology overview, concepts, ecosystem*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf>
- [23] *Technical Report FG DLT D1.3 Distributed ledger technology standardization landscape*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d13.pdf>
- [24] *Technical Report FG DLT D2.1 Distributed ledger technology use cases*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d21.pdf>
- [25] *Technical Specification FG DLT D3.1 Distributed ledger technology reference architecture*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d31.pdf>
- [26] *Technical Specification FG DLT D3.3 Assessment criteria for distributed ledger technology platforms*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d33.pdf>
- [27] *Technical Report FG DLT D4.1 Distributed ledger technology regulatory framework*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d41.pdf>
- [28] *Technical Report FG DLT D5.1 Outlook on distributed ledger technologies*. [Online]. Available: <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d51.pdf>
- [29] *Internet Research Task Force*. [Online]. Available: <https://irtf.org/>
- [30] *About Decentralized Internet Infrastructure (dinrg)*. [Online]. Available: <https://datatracker.ietf.org/rg/dinrg/about/>

- [31] *Meetings Decentralized Internet Infrastructure (dinrg)*. [Online]. Available: <https://datatracker.ietf.org/rq/dinrg/meetings/>[Online]. Available:
- [32] *Blockchain Governance Initiative Network (BGIN)*. <https://bgin-global.org/>
- [33] *About W3C*. [Online]. Available: <https://www.w3.org/Consortium/>
- [34] *W3C Blockchain Community Group*. [Online]. Available: <https://www.w3.org/community/blockchain/>
- [35] *Standards Australia Blockchain*. [Online]. Available: <https://www.standards.org.au/engagement-events/flagship-projects/blockchain>
- [36] Australian Department of Industry, Science, Energy and Resources (DISER), *THE NATIONAL BLOCKCHAIN ROADMAP: Progressing towards a blockchain-empowered future*. [Online]. Available: <https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf>
- [37] CEN – CENELEC *Artificial Intelligence, Blockchain and Distributed Ledger Technologies*. [Online]. Available: <https://www.cencenelec.eu/standards/topics/artificialintelligence/pages/default.aspx>
- [38] UNECE UN/CEFACT, *White Paper Technical Applications of Blockchain to UN/CEFACT deliverables, Version 2*. [Online]. Available: https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf
- [39] CEN – CENELEC *Work Program 2020*. [Online]. Available: https://www.cencenelec.eu/news/publications/publications/cen-cenelec_wp_2020_en.pdf
- [40] Simon Chandler, *What Is the Difference Between Blockchain and DLT?* 2019. [Online]. Available: <https://cointelegraph.com/news/what-is-the-difference-between-blockchain-and-dlt>
- [41] Alex Preukschat, *A Simple Guide to Understanding the Difference Between Blockchain and Distributed Ledger Believers*. 2018. [Online]. Available: <https://medium.com/@AlexPreukschat/a-simple-guide-to-understanding-the-difference-between-blockchain-and-distributed-ledger-believers-79cddccc8708>
- [42] Daniel Dob, *Permissioned vs Permissionless Blockchains: Understanding the Differences*. 2020. [Online]. Available: <https://blockonomi.com/permissioned-vs-permissionless-blockchains/>
- [43] Shermin Voghmir, *Token Economy: How Blockchains and Smart Contracts Revolutionize the Economy (English) (extract)*. 2019. [Online]. Available: <https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/>
- [44] Meg Cole-Adams, *Smart publications for smart contracts*. 2019. [Online]. Available: <https://www.standards.org.au/news/smart-publications-for-smart-contracts>
- [45] Charles A. Sennewald, Curtis Baillie, *Effective Security Management (Seventh Edition)*. 2020