ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

(1 AUG 2019)

ITU-T Focus Group on Application of
Distributed Ledger Technology
(FG DLT)

Technical Report FG DLT D5.1

Outlook on distributed ledger technologies

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

The ITU Telecommunication Standardization Advisory Group established the ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT) in May 2017.

FG DLT concluded and adopted its Deliverables on 1 August 2019.

Type	Number	Title
Technical Specification	FG DLT D1.1	DLT terms and definitions
Technical Report	FG DLT D1.2	DLT overview, concepts, ecosystem
Technical Report	FG DLT D1.3	DLT standardization landscape
Technical Report	FG DLT D2.1	DLT use cases
Technical Specification	FG DLT D3.1	DLT reference architecture
Technical Specification	FG DLT D3.3	Assessment criteria for DLT platforms
Technical Report	FG DLT D4.1	DLT regulatory framework
Technical Report	FG DLT D5.1	Outlook on DLTs

The FG DLT Deliverables are available on the ITU webpage, at https://itu.int/en/ITU-T/focusgroups/dlt/.

For more information about FG DLT and its deliverables, please contact Martin Adolph (ITU) at tsbfgdlt@itu.int.

© ITU 2019

Technical Report FG DLT D5.1

Outlook on distributed ledger technologies

Summary

This technical report is a deliverable of the ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT).

It explores the trends (e.g., technological and societal) in the field of distributed ledger technologies (DLT) which could lead to an evolution, or perhaps revolution, of these technologies as we know them today.

Keywords

Distributed ledger technologies; DLT; blockchain; data access; GDPR; ledger data structure; zero knowledge proof; programmability; consensus; identity; audit; legal perspective; token economy; sustainable development; locus of control; autonomous transactions, post-quantum cryptography, quantum resistant.

Disclaimers

(1) We were aware that the future is very difficult to predict when approaching this analysis of what technical, legal and business developments might impact the emerging information management technology called distributed ledger technology and vice-versa. Where innovation may emerge, and human ingenuity might introduce new capabilities, is hard to anticipate. As Lao Tsu said, "Those who have knowledge, don't predict. Those who predict, don't have knowledge." Acknowledging this challenge, we have attempted here to gather thoughts and insights on how this technology may develop and impact society over the coming years in order to provide some knowledge that will allow the reader to develop some understanding about the future of this technology, which can be used as input to their work and without pretention about actually predicting what will happen in the future.

(2) Token mentioned in this deliverable are only for the purpose of analysis of technical architecture and use cases. The Focus Group does not endorse any of these tokens, neither in the technical aspects nor as investments.

Name	Affiliation	Country	Email
Maranhão Suzana	BNDES	Brazil	suzana@bndes.gov.br
Mathis Angelo	PWC	Switzerland	angelo.mathis@ch.pwc.com
O'Brien Richard	Payment Pathways, Inc.	USA	rick@paymentpathways.com
Payen Patrice	Symantec	Switzerland	patrice_payen@symantec.com
Reis Taynaah	Moeda Seeds Bank	Brazil	taynaah@moeda.in
Ruffles Joseph	Clear	Germany	joseph@clearx.io
Schenker Inon	Impact Investments' Innovation	Israel	inon@singularititeam.com
Sylla Issa	IBM	USA	issa.sylla@ibm.com
Wang Dongyan	Tencent	China	alphawwang@tencent.com
Xiao Yue	University of Electronic Science and Technology of China	China	xiaoyue@uestc.edu.cn
Yong Chao	UESTC	China	yongchaomath@qq.com
Youm Heung Youl	Soonchunhyang University	Korea	hyyoum@sch.ac.kr

Editor: Dongyan "Alpha" Wang   E-mail: alphawwang@tencent.com
             Tencent
             China

CONTENTS

Technical Report FG DLT D5.1

Outlook on distributed ledger technologies

1   Scope

One of the key features that distinguishes human beings from all other creatures on earth is the capability to record as much history as they can in the past centuries and transfer knowledge to successive generations. This facilitates the human beings to be able to conquer some natural disasters, thanks to the record of the trial and errors and the ever-accumulated wisdom 'of the ages'.

This history has been recorded on stones, bamboos, clothes and paper, and stored in libraries from generation to generation. Nevertheless, this history is not complete. Inevitably, precious culture/experience/knowledge has been lost over the time span of human history.

Now, a cross-authenticated record of history is possible with more and more data able to be recorded thanks to distributed ledger technology (DLT) and artificial intelligence (AI).

Should DLT play important roles as data management requirements evolve? How will data access technologies be organized to address future requirements? This report attempts to summarize the existing work of SDOs and illuminate optimal paths forward.

DLT refers to the processes and related technologies that enable nodes in a network to securely propose, validate and record state changes (typically updates) to synchronize ledgers that are distributed across governance and jurisdictional boundaries. This document explores trends (e.g., technological, societal) affecting DLTs as we know them today.

The outlook on DLT is organized into five thematic clauses: Outlook 1-5. The nature of the outlook topics sometimes required multiple 'lenses' through which the theme could be viewed. Sub-clauses follow the structure of existing studies, future outlook and standardization roadmap.

Readers may scan and select different parts of the document which follows:
- **Outlook 1: Governance and legal regulation**
    a) Lays out the current picture of the legal framework;
    b) Analyzes liability in the context of decentralization; and
    c) Encourages a potential legal framework upgrade for sensible usage of smart contracts.
- **Outlook 2: Computation networks**
    a) How DLTs' inherent connectivity capability achieves high availability;
    b) Programmability and smart contracts;
    c) Ledger data structures for Peer-to-Peer (P2P) in DLT-based networks and their growth.
- **Outlook 3: Identity and privacy**
    a) Identity-proofing technologies required for sustainable resilience and how different trust models impact Know Your Customer (KYC), audit and risk management techniques;
    b) Privacy implications and instruments.
- **Outlook 4: Security and resilience**
    a) The key element of the context stamp to facilitate the resilient operation of DLT technology;
    b) The security level of consensus;
    c) Security verification of smart contracts;
    d) Quantum-resistant cryptography in DLT.
- **Outlook 5: Risk and audit**
    a) How risks and audit are related;
    b) Considerations on risk and audit in relation to DLT.
    c) Security and environmental aspects of DLT operations and how to balance risks.

2   Definitions

This document uses DLT related terms defined in ITU-T Technical Specification FG DLT D1.1 [b-DLT-D1.1].

3   Abbreviations

ABAC	Attribute Based Access Control
ABI	Application Binary Interface
AI	Artificial Intelligence
AML	Anti-Money Laundering
BFP	Bona Fide Purchaser
BTC	Bitcoin
CFT	Counter-Financing of Terrorism or Combating the Financing of Terrorism
CNIL	French data protection authority
CSP	Credential Service Provider
DAG	Directed Acyclic Graph
DAO	Digital Autonomous Organizations
DDoS	Distributed Denial of Service Attack
DLT	Distributed Ledger Technology
DPA	Data Protection Act
DPIA	Data Protection Impact Assessment
ERC	Ethereum Request for Comments
ETH	Ethereum
EVM	Ethereum Virtual Machine
FG DLT	Focus Group on Application of Distributed Ledger Technology
GDPR	General Data Protection Regulation
IAL	Identity Assurance Levels
IBFT	Istanbul Byzantine Fault Tolerant
ICO	Initial Coin Offering
ID	Identity
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
INATBA	International Association for Trusted Blockchain Applications
IoT	Internet of things
ITAS	Innovative Technology Arrangements and Services Act
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
KYC	Know Your Customer
MDIA	Malta Digital Innovation Authority Act

MRV	Measure, Report and Verify
NPM	Node Package Manager
PBFT	Practical Byzantine Fault Tolerance
PEP	Policy Enforcement Point
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PoA	Proof of Authority
PoS	Proof of Stake
PoU	Proof of Usage
PoW	Proof of Work
PQC	Post-Quantum Cryptography
PV	Peer Validation
RBAC	Rule-Based Access Control
RFC	Request For Comments
SDG	Sustainable Development Goals
SDO	Standards Development Organization
STO	Security Token Offerings
TX	Transaction
UNCITRAL	United Nations Commission on International Trade Law
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
VFAA	Virtual Financial Assets Act
UTXO	Unspent Transaction Output
VRF	Verifiable Random Function
ZK	Zero Knowledge
ZKP	Zero Knowledge Proof
zk-SNARK	zero-knowledge Succinct Non-Interactive ARguments of Knowledge
zk-STARK	zero-knowledge Scalable and Transparent ARgument of Knowledge

4   Introduction

The mission of this technical report is to explore the advancement of DLT technologies beyond legacy landscapes, frameworks, architectures, and through interaction with participants who are building the ecosystem. We hope that, by understanding what the latest trends imply, the standardization of DLT can proceed with prudence and coherence.

To encourage harmonization and consolidation among the many varied society requirements to enable operation at scale, we have analyzed intersecting dimensions of DLT:

- Societal expectations for sustainable development;
- Legal perspectives, policy and auditability to encourage healthy development corresponding to sustainable society expectations while respecting individual rights and freedoms;
- Risk manageability;
- Continuously evolving technical components to facilitate sustainable development, step by step.
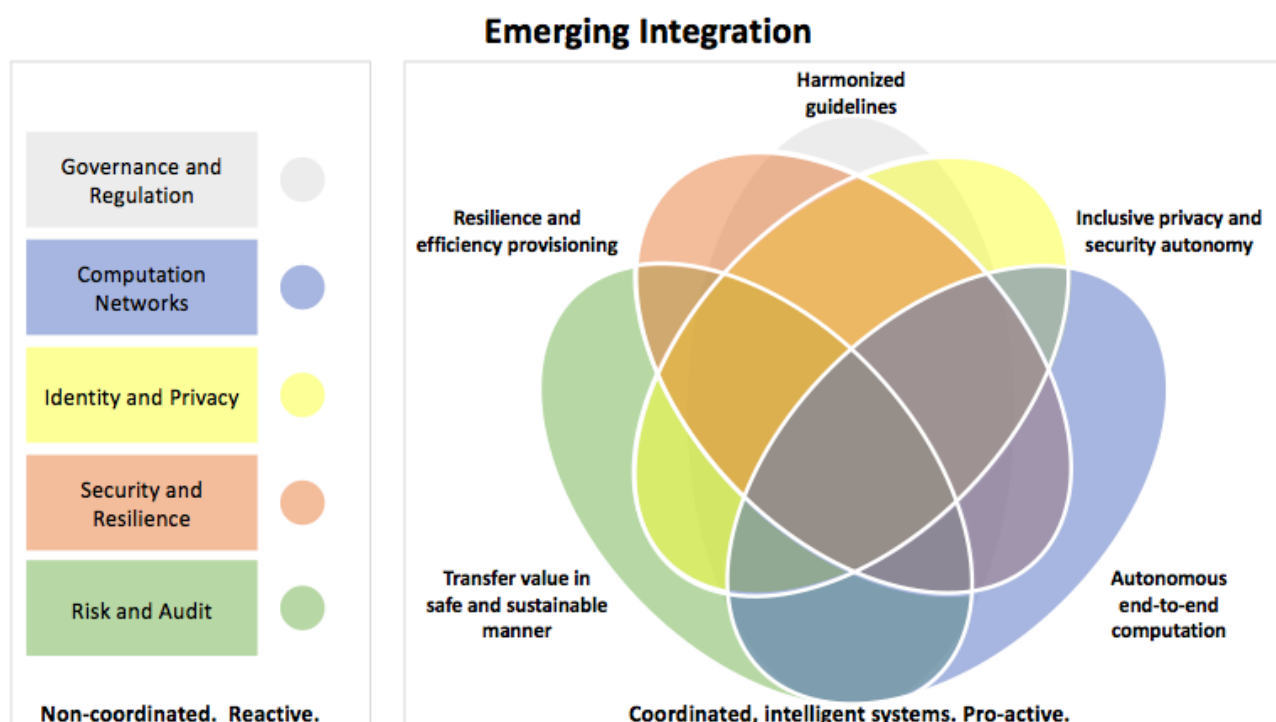
Figure 1: Surfaces of future considerations for emerging integration

Data is the basic element of industries and economies, today - the role of data will only become more central in the future. In Figure 1, emerging integration illustrates DLT technology development in a data-based economy. Users already take real-time service experience for granted, while current system architectures bear heavy burdens from ever-increasing transaction volumes. It has been observed that a bottleneck exists between streamlined processing in the daytime to meet real time requirements and multi-party verification in the night hours. With oceans of data being generated each second, it is challenging for the "night workers" to keep up with the "daytime workers", and thus a T+1 service loop is frequently utilized.

To provide efficiency during data processing, a consensus enabled, comprehensive, secure, and unalterable, data repository relieves the burden of document assembly between parties and saves time by consolidating document storage, reducing the risk of data loss and missing documents.

Does DLT enhance data processing efficiency and improve access control? DLT has been like a kaleidoscope with changing constellations of possibilities as described in ITU-T Technical Specification FG DLT D3.3 [b-DLT-D3.3]. ITU-T Technical Report FG DLT D2.1 surveys the DLT

landscape [b-DLT-D2.1]. Can we forecast DLT's future and minimize implementation risks upon review of the use case study in ITU-T Technical Report FG DLT D2.1 [b-DLT-D2.1]?

The major objectives of this report are:
- Take advantage of DLT's huge potential and disruptive impact, without compromising or impeding the constantly evolving set of regulatory and legal requirements;
- See where new technologies are shaping industries;
- Track unfolding legal and regulatory approaches across jurisdictions;
- Discover opportunities for standardization.

In summary, the target is to create a sustainable means of trusted information access and control in an environmentally friendly ecosystem under fair, coordinated control.

It has been said, "DLT has 'stirred the pot.'" Whatever the analogy, DLT has now stimulated innovators' imaginations!

We foresee many 'opportunities-for-improvements' by focusing our views of the environment, actors, and constraints through the lens of five demarcated systems.

It is important to know from whence, how, and why we came to embark on this journey. DLT provides

Figure 2: The objectives of DLT are to achieve the SDGs of the UN

the unprecedented opportunity for holistic thinking that could not have evolved under the separate governance constraints of demarcated systems.

The World Economic Forum's global risks report [b-WEF] addressed the growing number of complex and interconnected challenges from climate change and slowing global growth to economic inequality. The DLT outlook process is also an on-going consideration of the global risk landscape which drives investigations into varied cohorts in DLT contexts and how, together, we might solve the Sustainable Development Goals of the UN.

The challenges we are facing are not less compared to centuries ago:
- Are humans intelligent enough to conquer so many complex and interconnected challenges?
- Can a sparkling, vivid earth be passed on to everyone in subsequent generations, *endlessly*?
- Will new DLT methods record history in a manner that unveils yet unforeseen horizons?
- Will the DLT way to record history help us identify the *real* challenges as facts?
- Can trustworthy facts instrument corrective and preventative actions in a timely manner?
- Will the trust architecture that is DLT be feasible to sustain at scale?

5 Outlook 1: Governance and legal regulation

Governance and regulation have to ensure that we use distributed ledger technology in accordance with our values. While technology governance should foster sustainable development, individual freedoms must only be restricted where this is needed to prevent harm.

5.1 Governance and societal perspectives

GOVERNANCE AND REGULATION

Governance and Regulation
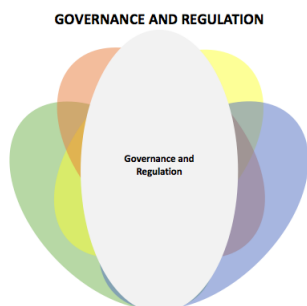
Around the world, governments and businesses are increasingly utilizing a "sustainability lens" on their core functions. How could DLT solutions change core functions and sustainability activities? What changes are needed to facilitate implementation at scale of DLT solutions? In the context of current and as well the future outlook for emerging sustainability issues (inter alia, climate change, global loss of biodiversity, plastic pollution in oceans), and also the calls to action recognizing the **scale, urgency, policy coherence and financial resources needed** to address these issues and to achieve the UN Sustainable Development Goals (SDGs), DLT and related digital solutions can have major impacts in many ways.

5.1.1 Existing studies

Trillions of dollars are needed to finance massive and urgent transformation of our economies and communities to be low-carbon emitting, climate impact resilient and to achieve the UN SDGs. Digital solutions, including DLT/fintech, are emerging that can support efforts to scale these financial flows and their development is the focus of the Task Force on Digital Financing for the SDGs established by the UN [b-UN-DF]. But, there are many challenges that impede sufficient flow of this finance, for example, the need for better data, information, standards, markets, policies and stakeholder partnerships. As with the UN task force for digital financing [b-UN-DF], the Task Force for Climate Related Financial Disclosures (TCFD) and many other initiatives across finance, government, business and civil society that have been established to address these challenges are not currently within a cohesive systemic strategy with well-coordinated actors and activities to operationalize a new open and integrated infrastructure to help finance the SDGs [b-TCFD]. In this regard, a recent report, Digital Momentum for the UN Sustainability Agenda in the 21st Century [b-WBGU], recommends the establishment of a 'UN Framework Convention on Digital Sustainability and Sustainable Digitalization'. Such new initiatives would complement ongoing efforts, such as the pan-UN "Atrium" initiative and other initiatives such as International Association for Trusted Blockchain Applications (INATBA), ConsenSys' Blockchain for Social Impact and the Climate Chain Coalition.

5.1.2 Future outlook

Although sustainability experts recognized early that the high energy demand of some DLTs was an issue to be resolved, they also quickly recognized that the benefits of DLT-enabled solutions in sectors such as finance and supply chains could be leveraged to enable positive transformation in our socio-economic systems and potentially achieve many sustainability goals.

Examples of how DLT-enabled solutions can help accelerate sustainability activities include:
- Supporting sustainable production systems, e.g., sustainable supply chains and product differentiation in commodity markets;
- Supporting sustainable consumption, e.g., digital currencies as smart money for "prosumers" and encouraging sustainable lifestyle behavior;
- Improving the transparency and credibility of sustainability claims, e.g., carbon footprint of a product, using measurement, reporting, verification (referred hereafter as: **Digital MRV**);

- Supporting sustainable finance (UN Task Force for Digital Financing for the SDGs), e.g., new ways to secure funding (equity or debt) for cleantech innovations and "ICT-smart" solutions, e.g., smart agriculture, smart mobility, as well DLT to track and manage sustainable finance;
- Supporting markets for environmental commodities, e.g., carbon credits, renewable power;
- Creating a "digital ecosystem for the environment" (UNEP), e.g., to track environmental data at the source as a "planetary ledger";

The world has tried for decades, with limited success, to create adequate solutions to the global sustainability crisis. It is not enough to recognize the many ways DLT-enabled solutions can be leveraged to support sustainability activities. The transformational change in socio-economic systems to achieve sustainable goals depends also on modernizing the system's tools to support DLT-enabled solutions. DLT-enabled solutions depend on good data, which depends on good governance and standards, especially in the context of sustainability, in order to Measure, Report and Verify (MRV) the environmental integrity and financial efficacy of effective sustainability activities. A major advantage of DLT-enabled solutions is the ability to internalize and automate, via smart contracts, the execution of procedures such as business and legal processes as well as MRV for sustainability.

5.1.3   Standardization roadmap

MRV for sustainability is a complex and massive system including countless methodologies, protocols, standards, guides, etc. MRV for sustainability currently involves many challenges – for example, in some cases there are no MRV procedures and in other cases there are conflicting MRV procedures. In short, the existing "pre-digital era" MRV system (inter alia, MRV procedures and the system of Standards Development Organizations (SDOs), is not aligned or synergistic with the emerging capabilities of DLT-enabled solutions. Therefore, the promise of DLT-enabled solutions to be leveraged within sustainability activities to enable the transformational change in our socio-economic systems to achieve the multitude of sustainability goals, requires a transformation in the existing supporting system of SDOs (e.g., to provide next generation rules for smart contracts). In other words, we need "Transformational Change" to be able to create the multitude (i.e., by a factor of 10 increase) of "DLT-ready" MRV procedures and at the same time reduce the cost and time to create these procedures by a corresponding (e.g., factor of 10) decrease.

Considering the human-centric processes of standards-setting, supporting technologies and new incentive mechanisms will be essential – and DLTs might offer a solution to this challenge as well by linking the standards-setting process with the use of smart contracts in the tokenization process of sustainability activities. Connecting these efforts with emerging work to develop collaborative platforms for smart contracts, such as OpenLaw [b-Open Law] among others, would help integrate governance innovation with digital innovation to support next-generation sustainability activities.

5.2   Applicable law and compliance for data assessment
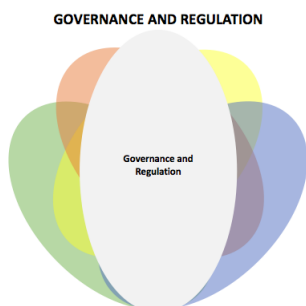
Clarity about the application of existing laws and drafting of new legislation provides legal certainty regarding the validity and regulation of DLT transactions. The DLT industry is gradually moving away from disruptive, but possibly non-compliant processes. This implies that legal innovation, while still lagging behind technological innovation, will catch up and require technological innovation to become compliant.

5.2.1 Existing legal regulations

DLT is far from being unregulated. Existing laws have to be respected. This is often a challenge because they were not made with DLT in mind. The global nature of most DLT-systems also means that systems have to cope with multiple jurisdictions.

5.2.1.1 Data protection: Privacy regulations

Privacy laws are being enacted in many countries. One of the strictest privacy law is the GDPR, which has been adopted in the European Economic Area. Due to its extraterritorial effect, European GDPR is an issue worldwide. A more detailed description on impacts of GDPR on DLT can be found in ITU-T Technical Report FG DLT D4.1 [b-DLT-D4.1]. Although the French data protection authority CNIL has voiced its opinion [b-CNIL] and the Blockchain Observatory at the EU commission has published a summary [b-EU Blockchain], we are still far from legal certainty. On the contrary, there are still many open points:

- Privacy Enhancing Technology (PET) is an effective means to provide privacy by design. However, in 2014 DPAs published an opinion [b-Art. 29 WP] with a very broad interpretation of what constitutes personal data. There is still legal uncertainty on how far privacy enhancing technologies like zero knowledge proofs or hashes will render data on blockchain anonymous. We expect the discussion to evolve here, during which some best practices on how hashing and other techniques should be applied to personal data might emerge;
- The GDPR distinguishes among three different roles: controller, processor, and data subjects. While data subjects are protected, the GDPR imposes obligations on controllers and processors. However, in many peer-to-peer applications – like public blockchains – many participants simultaneously take on several roles. Although the CNIL offers some guidance to determining the roles of participants, the peer-to-peer-nature of DLT-systems remains a challenge to the application of GDPR;
- The right to be forgotten and the right to erasure are not absolute rights. There can be justifications to continuous data storage even when the data subject asks for its deletion;
- Due to the immutability of blockchains and the use of privacy enhancing technologies, privacy has to be taken to account by design. Data Protect Impact Assessments (DPIA) are frequently required.

5.2.1.2 Token economy

Raising funds by selling tokens has been one of the dominant uses of DLT. The Securities and Exchange Commission (SEC) in the US now classifies most tokens as securities [b-SEC]. The successful injunction in the case of Blockvest BLV tokens [b-Todd] does not seem to reverse that rule. China is also taking a strict approach [b-Maloney]. Easy fundraising through tokens seems to be over. Chilling effects might even lead to stricter compliance than IPOs.

Currently, countries are beginning to enact specific legislation concerning ICOs, STOs and the token economy: Gibraltar has passed a DLT regulatory framework [b-GFSC]. Malta has passed three new laws, which introduce certification requirements for ICOs [b-Malta-a, b-Malta-b, b-Malta-c]. In Liechtenstein, a new law has been passed [b-Liecht] and Switzerland has published a Federal Council report [b-Swiss]. Other countries have clarified how existing laws apply to ICOs and STOs.

5.2.1.3 Regulation on identity services

Currently, laws on digital signatures, electronic identification, and trust services like the European eIDAS are often not technology neutral and do not include DLT. Some courts are beginning to accept hashes on blockchains as legal evidence [b-Rhodes]. New laws on electronic identification and trust services will probably support the use of DLT-based evidence in court.

5.2.1.4 Liability of participants

One of the main characteristics of most DLT is that node operators have little to no influence on the content they store on their node. In telecommunication law, we know a legal institute called "provider privilege" – for example, in directive 2000/31/EC [b-Choudhury], provider privileges differ among providers:

- Those that merely do the transmission;
- Those that do some caching;
- Those that provide hosting services.

While a hosting provider has the obligation to remove illegal content upon notice, a blockchain node cannot remove some content and at the same time remain a valid node. The scope of liability of node operators, miners and other blockchain participants still needs clarification. Regarding GDPR, the European regulation distinguishes between controllers and processors and imposes a reduced liability on processors. The French data protection authority CNIL regards blockchain nodes of public blockchains as processors and hence reduces their liability.

5.2.2 Future outlook

Existing regulation will be clarified, often tightened, and new regulations will be created.

5.2.2.1 Data protection

We will have to see whether data protection authorities from other EU countries will agree with the interpretation of the CNIL. We expect some points to be settled soon. However, some concepts of DLT and GDPR are too different for easy solutions. Since DLT in combination with privacy enhancing technology is often used to provide privacy by design – something data protection laws are also aiming for – data protection laws should accept DLT as a possible tool to achieve good privacy.

5.2.2.2 Token economy

ICOs, TGEs and STOs have been the dominate use-case for tokens. Starting almost without any regulatory interference, regulations do increase with compliance requirements getting similar to those for IPOs and other financial instruments. We expect that we will have tighter regulation, which will also bring more legal certainty here. Access to tokens markets might be restricted to jurisdictions where compliance has been positively ensured. Transferability of tokens might be restricted in order to ensure compliance.

Tokenization goes further than investment funding. Property, rights and other assets can be tokenized.

An important precondition for the token economy is the finality of token transfers. When tokens represent a share or another right, the token must not be disconnected from the right. A Bona Fide Purchaser (BFP) needs to be protected in order to create trust in the tokens. Other countries might follow the example of Liechtenstein and will adapt laws to regulate the finality of token transfers.

5.2.2.3 Identity services

Proofs of identity, timestamps, contracts and certificates based on blockchains will become commonplace. Blockchain-based proofs will increasingly receive legal recognition by courts and lawmakers.

5.2.2.4 Liability of participants, governance

DLT systems and smart contracts provide trust through their decentralized architecture. No single institution or operator can change information stored on a decentralized ledger. Smart contracts are executed as code and stored on the ledger. However, software tends to have bugs, smart contracts

might not foresee everything that can happen, and the legal evaluation of a contract can change. Conflicts must be resolved and software needs to be updated. To preserve the decentralized structure of DLT systems, any kind of conflict resolution and governance needs to be decentralized. Every DLT system and every smart contract therefore needs to include some kind of decentralized self-governance.

Standards for the self-governance of DLT systems shall be developed in the coming years. When a DLT system provides a sufficiently complete, independent, and robust system of self-governance that respects the rule of law, legal authorities like courts will respect its decisions. This can be compared to the respect of decisions by arbitral institutions as laid down in the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards [b-New York]. International trade organizations like UNCITRAL could be a good forum to develop these standards.

It remains to be seen how far governments will include node operators in the provider privilege and whether nodes will be forced to exit a chain if they cannot otherwise remove some illegal content. With the creation of governance structures their liability also has to be determined.

5.2.2.5 Restrictions on mining

Environmental impacts of blockchain mining might increase. Due to its power consumption, mining is currently banned in some countries. Other countries might follow or act through special tax regimes. However, since most new DLT systems do not rely on proof of work (PoW), the impact of these restrictions on DLT will be limited.

5.2.3 Standardization roadmap

Most DLT systems involve actors and nodes in different countries. Cross-border disputes on a transaction-by-transaction basis might prove to be inefficient and inconsistent. Therefore, uniform international rules are desirable. Among topics to be addressed are the limitation of liability of node operators as well as the recognition of decentralized self-governance of DLT systems and smart contracts.

Pre-standards and standards currently being developed by SDOs are an important precondition to provide legal certainty. DLT-related standardization activities (including from ITU-T, ISO, IEEE Standards Association, W3C, UN/CEFACT, UNCITRAL, ETSI, CEN/CENELEC, NIST, DIN, and other communities) are described in more detail in ITU-T Technical Specification FG DLT D1.3 [b-DLT-D1.3].

On top of that, model laws and international conventions could be developed to provide legal certainty.

6   Outlook 2: Computation networks

Computation and data repositories have become increasingly available everywhere, even in places without network access. Digital technology permeates nearly every aspect of our lives. Understanding the many dimensions of computation networks can accelerate sustainable development in a manner that is safe, speedy, and practical.

6.1   Connectivity capability and high availability
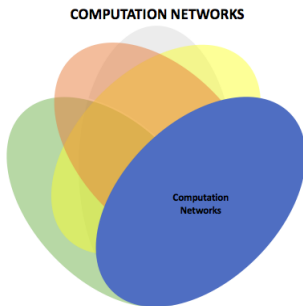
Resilient electrical power and network connectivity cannot be regarded as givens in every circumstance where DLT nodes are operated. Identification of potential drawbacks can isolate risks. Improvements must advance beyond Proof-of-Concept and become operating baseline solutions.

6.1.1   Existing studies

The communication and verification mechanism of P2P jointly constitute the cornerstone of the blockchain network. By observing three major streams of blockchain systems, Bitcoin [b-Nakamoto], Ethereum [b-Ethe-a, b-Ethe-b] and Hyperledger fabric [b-Hyperledger], the typical P2P organization can be categorized into three main types:

- Decentralized unstructured topology (e.g., Bitcoin)
- Decentralized structured topology (e.g., ETH)
- Partially decentralized topology (e.g., Fabric)

In Table 1, P2P network, also as a function of blockchain, is analyzed and compared – because the quality of network determines the success of blockchain products.

Table 1: P2P network topology comparison

P2P topologies / Comparison criteria	Centralized topology	Decentralized unstructured topology	Decentralized structured topology	Partially decentralized topology
Scalability	Poor	Poor	Good	Medium
Reliability	Poor	Good	Good	Medium
Maintainability	Best	Best	Good	Medium
Node access efficiency	Highest	Medium	Poor	High
Security	Best	Medium	Medium	Good
Private protection	Medium	Best	Good	Good

Network architecture design is particularly important for blockchain, and the mentioned applied topologies all have some inevitable shortcomings. Decentralized networks outperform centralized networks in scalability and flexibility, offering effective approaches for large-sized communication scenarios. Indeed, more nodes, means more copies, which slows down the network. This is why centralized blockchains like Ripple can achieve better performance with only 55 validator nodes. However, decentralized networks are incapable of optimizing real-time performance and reliability based on local information, affecting the performance of connectivity capability and availability. By contrast, centralized networks can rely on complete information to improve both types of performance. To this end, a hybrid network architecture might allow a tradeoff among network

performances, salability, and flexibility. Additionally, many of the leading cryptocurrencies have hit a wall in terms of scalability in real world use. Therefore, much effort from industry and the research community is devoted to the design of blockchain scaling methods that address lower latencies and higher throughputs. The table below illustrates the features of the various solutions.

Table 2: Comparative study on scalability

Solutions	Claimed TPS	Layer	Platform	Potential drawback	Notes
Casper	50 [b-Schmid]: in the premise of that the failure type of a node only considers that the node sends a self-contradictory message.	Layer 2 (off-chain) [b-Zamfir]	ETH [b-Croman]	An ever-increasing risk of oligarch in the network occurring	Ethereum's main scaling goal. Casper is the shift from PoW to the more efficient PoS.
Plasma	5000 [b-Schmid]	Layer 2 (off-chain) [b-Poon]	ETH [b-Croman]	Everyone using a child-chain tried to exit the sidechain at the same time may incur the assets loss.	The intro of "child" chains off the main Ethereum blockchain for faster and cheaper transactions. Similar to how the Lightning network works on Bitcoin.
Sharding	45000 [b-Schmid] there are several levels of nodes: super full node, top node, single slice node, and light node.	Layer 1 (on-chain) [b-Drake]	ETH [b-Croman]	Data availability and fraud detection	Partition the existing blockchain into smaller pieces known as shards.
Raiden red eyes	1000000 [b-Schmid]: in the premise of micropayment.	Layer 2 (off-chain) [b-Mission]	ETH [b-Schmid]	Cannot guarantee the security of large transactions.	Off-chain solution for faster and cheaper transactions
Bloxroute	200000 [b-Klarman]: in the premise of that minors run gateway nodes.	Layer 0 [b-Klarman]	ETH [b-Klarman]	An ever-increasing risk of forks in the network occurring and the blockchain unraveling.	An optimized, well-provisioned global distribution network, deploying its own servers worldwide to achieve this.
Lightning Network	Millions [b-Lightning]: in the premise of micropayment.	Layer 2 (off-chain) [b-Peach]	BTC [b-Peach]	Cannot guarantee the security of large transactions.	The implementation of HTLCs with bi-directional payment channels which allows payments to be securely routed across multiple peer-to-peer payment channels.
Liquid network	Millions [b-Liquid] premise: all participants on network accept updates on the network, and no entity can control multiple Liquid Network servers.	Layer 2 (off-chain) [b-Preiss]	BTC [b-Preiss]	Not applicable to decentralized or P2P payments.	A Bitcoin sidechain "provides fast, secure, and confidential transactions to address the needs of exchanges, brokers, market makers, and financial institutions around the world."

6.1.2 Future outlook

From connectivity perspectives, advanced networking is the unsung hero of DLT future, offering a continuum of connectivity that can transform inefficient DLT operating models. Next-generation technologies and techniques such as 5G, low earth orbit satellites, mesh networks, edge computing, and ultra-broadband solutions promise order-of-magnitude improvements that will support reliable, high-performance communication capabilities; software-defined networking and network function virtualization help companies manage evolving connectivity options. Based on these connectivity building blocks, a hierarchical management structure illustrated in detail in figure 3.
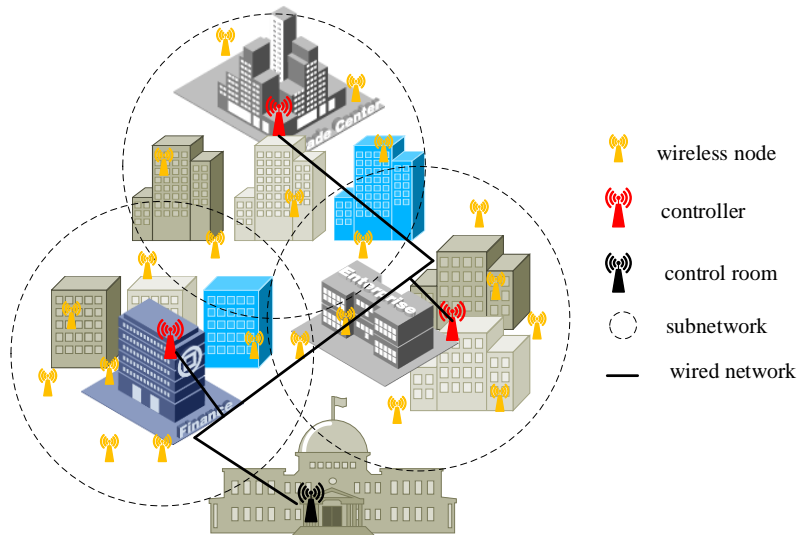
Figure 3: Hierarchical framework

As shown in figure 3, a hierarchical network contains controllers (i.e., pool managers), mobile nodes, and actuator nodes. A subnetwork controller and some surrounding nodes constitute a subnetwork, and a controller only corresponds to a subnetwork. In this network architecture, it is proposed to integrate wireless communication into blockchains. Moreover, using advanced networking can not only support mobile blockchain nodes, but also significantly reduce the cost of future network infrastructure.

From scalability perspective, the hybrid schemes with tradeoff between centralization and decentralization could adapt the rhythm of human society growth, thus more practical in near future.

6.1.3 Standardization roadmap
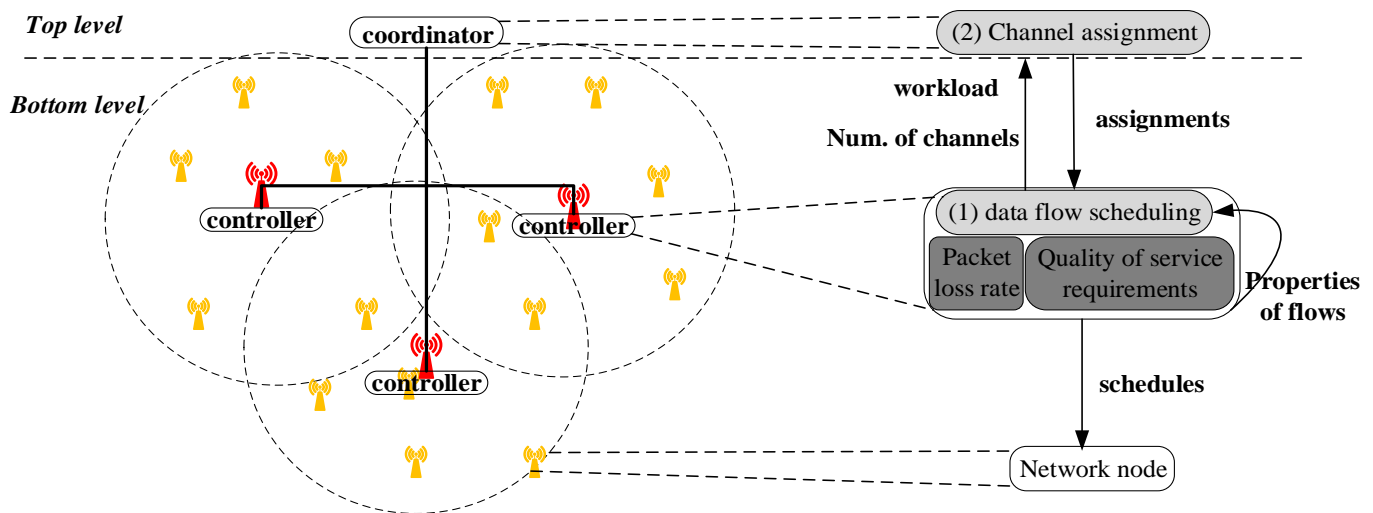
Figure 4: Hierarchical management framework overview

The existing schemes presume that the network is with unlimited capacity to accommodate variant transactions; while as we know this could be the bottleneck for the performance improvement.

Based on the hierarchical network shown in the above figure, the performance improvement of reliability of transaction data and transmission latency can be realized mainly by the proper use of communication resources, including the transaction flows scheduling in the bottom level and the radio blocks allocation in the top level.

The standardization roadmap could be as follows:

- A hierarchical framework to facilitate managing the communication resources, the hierarchical framework manages different-grained resources on multiple levels.
- Level and subnet specific control domain. The network domain controller manages the traffic flows in its subnetwork.
- Coordinator level schemes.

From scalability perspectives, the standardization of the interface between the centralized systems could be a way forward to balance the performance and interoperability?

6.2 Programmability and smart contracts

6.2.1 Existing studies
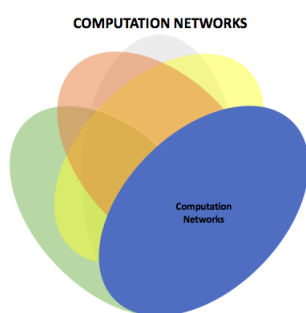
The 'smart contract' is one of the capabilities that has been introduced in DLT ecosystem. While still limited in capability and generally insufficient for practical usage in real society operations, vast resources are being invested to develop experimental methodologies for enhancing programmability and effectiveness, dependence, hierarchical, defect corrections mechanism, lifecycle and evolution.

6.2.1.1 Virtual machine

Improvements to virtual machines are advancing DLT programming capabilities. One such improvement is WebAssembly.

WebAssembly (abbreviated Wasm) is a binary instruction format for a stack-based virtual machine. It will enable high-performance web apps for applications such as computer-aided design and video and image editing. Web apps written with WebAssembly can run at near-native speeds because, unlike JavaScript, codes programmers write are parsed and compiled ahead of time before reaching the browser. The browser then just sees low-level, machine-ready instructions it can quickly validate, optimize and run. Currently there are compilers for C, C++ and Rust.

Major browser JavaScript engines will notably have native support for WebAssembly, including but not limited to: Google's V8 engine (Node.js and Chromium-based browsers), Microsoft's Chakra engine (Microsoft Edge), Mozilla's Spidermonkey engine (Firefox and Thunderbird). Other non-browser implementations exist too: wasm-jit-prototype (a standalone VM using an LLVM backend), wabt (a stack-based interpreter), ml-proto (the Ocaml reference interpreter), etc.

Some DLTs groups are executing projects to support an adaptable version of Wasm, such as the eWasm project of Ethereum and the EOS platform. Besides the advantage of supporting many high-level languages, a community of a DLT using WebAssembly EVM could take advantage of a broader tooling compatibility.

6.2.1.2 New generation of programming languages

Programming languages are being developed targeting DLT platforms considering lessons learned from existing technologies. Their use may help to make smart contracts more secure and easier to develop and test.

For example, Vyper is a new language for the Ethereum platform (beta tested in June 2018) that is focusing on the delivery of security, human readable code and language and compiler simplicity. This language is not trying to be a replacement for Solidity. Both languages can coexist. Vyper is a subset of Python syntax and implements the following features: decidability – reliably compute upper bounds for gas consumption (gas is a unit of measuring the computational work of running

transactions or smart contracts in the Ethereum network) of any function call, small and understandable compiler code, strong typing, bounds and overflow checking, support for signed integers and decimal fixed-point numbers and limited support for pure functions. Vyper does not support function modifiers, class inheritance, inline assembly, function overloading, recursive calling and infinite-length loops.

From third parties other than DLT platform providers, several new cross-platform languages have been proposed. Examples include:

- Simplicity is a strongly-typed combinator-based low-level language that features analysis of resource usage on virtual machine. Primarily owing to its Turing-incompleteness, temporal and spatial boundaries of resource use can be estimated by static means;
- Ergo is another strongly-typed functional language that has platform-independent semantics. Similar to Simplicity, it also imposes a restriction on iterations and guarantees termination of contract execution [b-Ergo].

For the initial release of Hyperledger Fabric in 2016, the Linux Foundation implemented the blockchain platform's smart contract Golang, capitalizing on Google's fast, easy-to-learn, strongly statically typed language.

6.2.2 Future outlook of programmability and smart contracts

Smart contracts, written in a multitude of programming languages, are the driving mechanisms within blockchain technologies. As of 2019, several blockchain frameworks rely on smart contracts to define the underlying business logic. Embedded within the network, these encoded rules govern transactions, ensuring consistent data across the environment. Whereas, the programmability capability may expand with the scope of its usage into variant options in the future, the trend could be further accelerated with the progress of the smart contract.

Additional information can be found in Annex A.

6.2.3 Standardization roadmap

Several technical standards are emerging in order to facilitate code development and minimize bugs. For example, in the Ethereum platform there are: ERC-20/ERC-777 (Fungible Tokens), ERC-721 (Non-Fungible Tokens), ERC-809 (Renting Standard for Rival, Non-Fungible Tokens).

These standards help to create a common understanding of the source code of smart contracts and to develop the ecosystem. For example, many ICOs that have been launched until now use the ERC-20. It became simpler to create fungible tokens after the standard ERC-20 and it probably increased both the number of new ICOs and the number of people willing to invest in this way of funding.
Some works are trying to abstract domain requirements and to create smart contract templates, which can be instantiated according to real use cases needs [b-Choudhury].

6.3 Ledger data structure

COMPUTATION NETWORKS
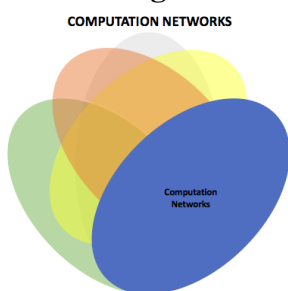
Ledger data structures (e.g., directed acyclic graph (DAG), linked list) are very tightly coupled to consensus protocols. However, this fact does not imply that they will remain so tightly coupled in the future. Future outlook is keeping it in view.

6.3.1 Existing studies

Decentralized ledger technologies, in the most abstract terms, aim to achieve consensus amongst a group of untrusted nodes about states (binary strings) and about transitions to those states, which fulfill certain validity rules agreed by the group.

DLTs should therefore achieve the following regarding state and transactions:

- Validity of initial states;
- Consensus regarding state transitions in the face of malicious actors and byzantine nodes;
- Ability to execute valid transitions in the face of malicious actors and byzantine nodes;
- Availability of state and transition information for participants.

DLTs achieve these goals by a combination of a consensus algorithm's deterministic validity rules and availability incentives.

To implement this combination, a ledger data structure may contain:

- Information about states;
- Information about included valid transitions;
- Information as per the consensus algorithm to determine consensus on transactions, states and transitions.

This structure may be a concretely stored structure stored by all nodes – however, in practice and in most cases, it is more efficient to store only parts of the ledger data structure, along with supporting data to efficiently validate specific states without processing all intermediate transactions. When this method is chosen, the efficient supporting data is usually incorporated into the consensus state to increase its availability and is generally considered part of the ledger data structure.

There is a range of implemented ledger data structures, and more are under active development. Due to the tight coupling between consensus algorithms, states, validity rules and ledger data structures, it is not usually possible to mix-and-match ledger data structures with consensus algorithms. However, some consensus algorithms families do share similar ledger data structures and may be used interchangeably (e.g., Nakamoto consensus and PBFT).

When comparing ledger data structures, the following parameters may be used to compare structures and find their fit to specific use-cases:

- Storage size and growth – As a DLT is in operation its ledger data structure will grow as new transactions and state transitions occur. Different data structures have different properties regarding the amount of data from the ledger data structure that must actually be stored on nodes to participate in the DLT. This may range from a linear growth (like in Bitcoin) to a fixed size (like in Corda or Grim);
- Availability requirements for transition – As not all of the ledger data structure may be stored in each participating node, or be required for participation in consensus, it is important to consider availability requirements for creating transitions. For example, in privacy-oriented DLTs clients must usually store supplementary information per each unspent transaction to allow them to "spend" those transactions (vs non-private UTXO-based DLTs in which a client can scan the list of transactions to identify owned transactions);
- Strength of ordering – While almost all DLTs maintain some ordering between executed transactions, not all DLTs maintain a strict strong ordering of transactions when one is not required for validity (e.g., between two transactions which do not reference any shared account);
- Cost of initial bootstrap – Different ledger data structures require different amounts of processing to validate and build data structures required for participation. When supplementary data is provided this processing can be reduced, however, there is usually a tradeoff with availability requirements.

Table 3: Common families of ledger data structures in use or development as of August 2019

Name	Structure	Storage size and growth for a validating node	Availability requirements for running a validating node	Availability requirements for transaction creation	Strength of ordering
Bitcoin blockchain	Hash-chained blocks of transactions	All transactions grow linearly	Block headers, Full UTXO set	Relevant unspent transaction outputs	Total, all transactions are ordered
Ethereum blockchain	Hash-chained blocks of transactions	All transactions grow linearly	Block headers, full state structure	State sub-structure relevant for transition	Total, all transactions are ordered
Tangle	DAG of blocks	All transactions grow linearly	All transactions. You can partially validate with partial data	Two older valid transactions, although for rapid transmission and verification, these should be in the "heaviest" branch	Partial, based on which transactions are "ancestors"
Fixed-length	Account table and fixed verification string	Accounts only, grows by # of accounts (not TXs)	Fixed verification string, UTXO set	Relevant unspent transaction outputs	Total (In most implementations)
Sharded / parachains	Multiple hash-chained blocks of transactions with some relationships	All transactions grow linearly	As required by shard type, most nodes validate only a subset of all shards.	As required by shard type, only "shards" or "chains" participating in transaction	Total for each chain, with "cross-links" to create ordering between chains
Block lattice	Per-account hash-chained transactions	All transactions grow linearly	Nodes validate certain accounts only, and only need the relevant history for that account and accounts it interacted with	Consensus state for accounts participating in transaction	Partial - Accounts have total order, unrelated accounts unordered
HashGraph	DAG of blocks	All transactions grow linearly	All transactions	Two older valid transactions	Total, all transactions are ordered

6.3.2 Future outlook

While a number of different distributed ledger technologies have exploded in recent years, in practical applications (e.g., telecommunications) customers who want to exploit their power still want some choice of vendor and technology to meet their specific requirements (and to promote innovation and control cost). Organisations who participate in various consortia regularly ask for inter-DLT interoperability – which will drive innovation in this direction.

6.3.3 Standardization roadmap

As and when interoperability between chain technologies (and chain instances) becomes a reality, it will happen via some level of standardization – an obvious opportunity for the appropriate standards setting organizations.

7   Outlook 3: Identity and privacy

Identity and privacy, given the exponential growth and impact of digitalization in our daily lives, are topics that receive our attention to secure autonomous control of one's privacy and confidentiality.

7.1   Identity and KYC
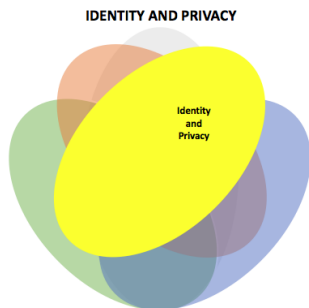
Today's accrediting bodies for education, healthcare, accounting, banking, product testing, public safety, etc., are centralized and fragile. This implies that the fragility of hierarchical systems stems from a presumption of trust in the root. The premise that singular authorities are the best way to anchor trust is now challenged by alternatives presented by DLT. Systems are emerging that encourage one to get second opinions or measure direct results with autonomy. Such systems have functions that evaluate evidence in the background.

7.1.1   Existing studies

Partial list:
- Identity Management Sub-Committee (IMSC) Pan-Canadian Trust Framework [b-IMSC];
- eIDAS (electronic IDentification, Authentication and trust Services) is the EU regulation entered into force on 17 September, 2014 instituted the first significant set of standards of electronic identification and trust services for electronic transactions in the European Single Market;
- NIST report - Issuance (credential management) and identity authentication [b-Grassi];
- US Federal Reserve report - Risks of synthetic identity fraud in payments [b-US].

7.1.2   Future outlook

By adhering to the guidelines set for technology under proposed frameworks such as IMSC's proposed Pan-Canadian Trust Framework and early legislation such as eIDAS, we project the future should achieve higher levels of information security and innovation in identity and KYC.
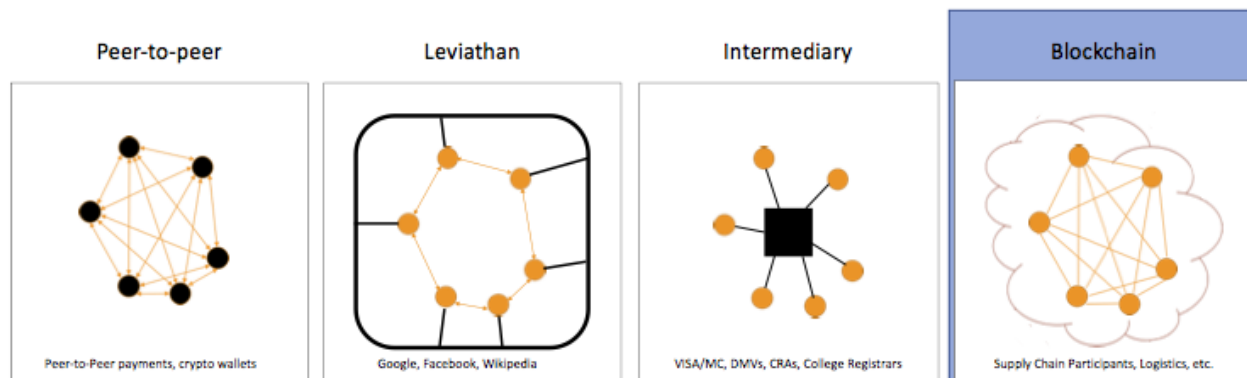
The blockchain's "trustless" trust architecture, promoting trust in the network without trusting any individual actor, compared to alternatives

Figure 5: **The trust challenge [b-Werbach]**

Certain DLT models create a new kind of trust than none of the established models encompass. ITU-T Technical Report FG DLT D4.1 [b-DLT-D4.1] and this future outlook express the need for further study to define and identify governance and rules gaps. Simply put, we assume legacy trust models will continue, and with the arrival of different kinds of DLT-based trust frameworks, the mere adjacency of disparate systems requires identification gaps in:
- Rules (e.g., for legal enforcement);
- Identified entities positioned to address challenges;

- Alignment of resources and incentives necessary to solve the trust challenge.

To narrow these gaps, we recommend focus be applied to the following:
- *Interoperability*: Desired outcome for DLT is to create a common gateway protocol for data exchange among different trust frameworks. We recognize that electronic IDs from DLT systems that operate under different governance structures must ensure its authenticity and security. The desired outcome: make it easy for users to conduct business across borders.
- *Transparency*: Desired outcome for DLT is to provide a clear and accessible list of trusted Identity Proofing services that may be used:
  - i) Within a given centralized signing framework, or
  - ii) With complete autonomy, allowing for entire new trust frameworks based on DLT as described by Kevin Werbach (see above diagram).
- *Autonomy (a.k.a. Self-agency – Intentional authorization)*: The network is where we find our digital information. Often, we rely on centralized or federated entities to protect the confidentiality, integrity, and access to digital information. As new technologies shift processing resources nearer to data sources, a way to augment protections in a decentralized manner may render some external dependencies unnecessary. Autonomous Transactions achieve outcomes faster, with less risk, and with superior accuracy with less complexity
- *End-to-End Principle*: Mobile programs do not operate in a static environment. *"Mobile programs are capable of moving in the internet environment to fulfill queries received from users, including from other programs, and to integrate information received with other communications in order to provide a reply. ... In order to anticipate the integration of certain advanced and/or rapidly evolving technologies, the definition of the internet must be broadened to recognize the need for flexibility and implementation for the future."*

To achieve easy-to-maintain and effective cyber-security, smartphone owners need a tool to prove and protect self-agency. This boosts achievement of economic autonomy and is unstoppable.
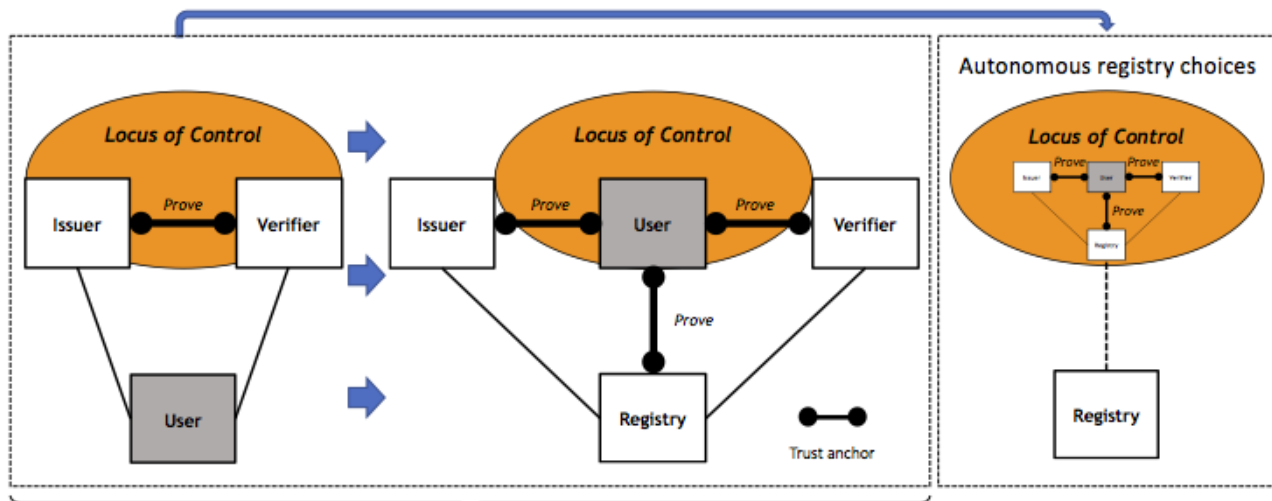
Figure 6: Locus of power and control [b-Bouma]

New computational tools will construct autonomous validity proofs for:
- A natural person's attestation of accuracy for claims that comprise an entity's identifiable characteristics;
- A natural person's intent to activate processes to affect the transfer, storage and retrieval of informational and/or monetary assets;
- The use of resolvable variables in process equations that affect the transfer, storage and retrieval of informational and/or monetary assets.

Such tools extend the power of DLT-based registries to include structured digital objects known as rules, algorithms or process instructions (a.k.a. smart contracts). Precision software tooling extends

the scope and usage of process instructions to a broader range of informational and/or monetary asset transfer transactions by mitigation or outright elimination of certain execution risks.

By extending the reach of trustworthy data validation services by the enrollment and persistent refreshment of autonomous proofs of data validity to one or more identification registries (i.e., blockchain/DLTs). Data that can prove and protect its trustworthiness with regard to integrity (accuracy), confidentiality (access) and privacy (usage) presages new classes of machine-to-machine use cases.
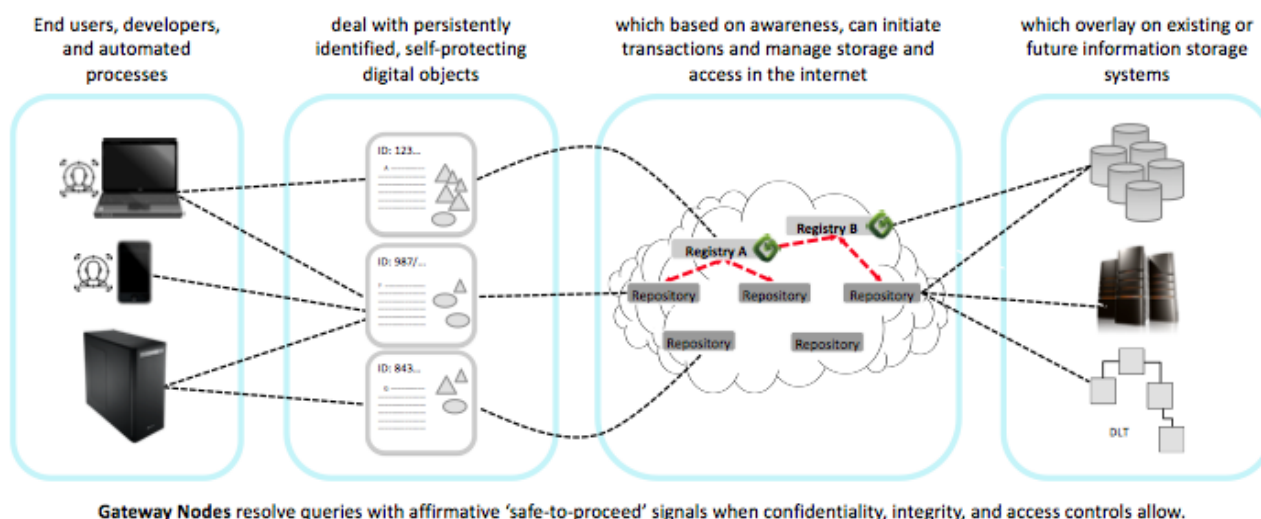
Figure 7: Autonomous transactions [b-CNRI, b-Lyons]

7.1.2.1   Identity and KYC in DLT

Naming transacting digital content and other representations of stored value (e.g., fiat and non-fiat virtual currencies, alike) require transacting entities to have names denoting specific referents. Binding an attribute to a digital object is the deterministic method that constructs the "named identity" to Who, What and How entities. 'Who-entity' names may be pseudonymous and unique. Anonymity and ambiguity are explicit non-goals of Know Your Customer (KYC).

The identity lifecycle of a Who-entity is a process that starts when a person applies for a digital ID and ends when the record is removed, and the ID is invalidated owing to death, request for removal by the individual, or some other event.

Activities take place during the lifecycle and may be recorded on:
- a blockchain;
- an off-chain mechanism; or
- a sidechain. For example, Authorization, (i.e., an act of agency) can be implemented and enforced by relying parties.

Registration (identity proofing). Applicant entities provide evidence of connected attributes to a credential-issuing authority. If the person proves attribute bindings that comprise his or her 'identity', the authority can assert that 'identity' with a certain level of identity assurance. In cases like those of displaced persons or refugees, it is not uncommon for applicants to lack fundamental documents (birth certificate, passport, utility bill, driving license). In some situations, even if a birth certificate is available, it may not be trustworthy.

In such circumstances, identification systems may use an 'introducer' who is tasked with verifying the applicant's identity and address. Once verification is completed, biometric registration and de-duplication will bind the applicant to his or her identity claim, which will then be used during subsequent identity interactions. Ideally, a digital identification system should be integrated with civil registration, which is the official recording of births, deaths, and other vital events including

marriages, deaths, divorces, annulments, separations, adoptions, legitimations, and recognition. What this means in practice is that a person's record in the digital ID system and his or her unique ID number are first generated through registration of their birth. The digital ID system is notified of a person's death as soon as possible after death registration. Aside from promoting coverage and sustainability of a digital identification system, this integration provides an opportunity to produce real-time vital statistics, such as on population, fertility, and mortality.

Registration may start with resolution, the process of uniquely distinguishing an individual in a given context. The first step in resolution is pre-enrollment when the applicant provides the issuing authority with biographic information, breeder documents (such as birth certificates, marriage certificates, and social security documents), and photographs. The applicant can present these in person or provide the information online or offline. This is followed by enrollment, which typically happens in person, so pre-enrollment information can be validated and augmented by the registration authority as needed.

In-person proofing is required for the highest Identity Assurance Level (IAL) [b-Drummond, b-Jain]. When the demographic and biometric information is validated and enrolled, identity proofing typically continues with de-duplication to ensure that the individual did not register under a different claim of identity.

This can be accomplished with an identification (1: N) search of the entire biometric database using one or more biometric identifiers (physiological and/or behavioral characteristics that are used to identify an individual). This process can be especially challenging with large populations.

Validation is where an authority determines the authenticity, validity, and accuracy of the identity information the applicant has provided, relating it to a living person. Verification establishes the link between claimed attributes of an identity and the real-life subject presenting the evidence. Vetting/risk assessment assesses the user's profile against a watch list or a risk-based model.

Identity proofing is the process whereby an authority:
- Resolves a claimed set of identity attributes to a single, unique identity within the context of the population of users that the Credential Service Provider (CSP) serves;
- Validates that all supplied evidence is correct and genuine (that is, not counterfeit or misappropriated);
- Validates that the claimed set of related identity attributes exists in the real world;
- Verifies that the claimed set of identity attributes is associated with the real person supplying the 'named identity' evidence.

For developing countries, multiple challenges may arise during the registration process:
- The hardware and software used for registration activities needs to be accurate, affordable and usable;
- The system must be inclusive. Some individuals may have poor biometric features (like poor fingerprint ridge structure) that make accurate enrollment difficult;
- The presence or absence of an assignment and acceptance of liability for the accuracy of an authority's attestation of attribute bindings by an authoritative Credential Issuer becomes a mandatory requirement when credentials are stored to a blockchain system for verification purposes.

7.1.3 Standardization roadmap

In the society of human beings, identity assists resource allocation in the trust oriented economic process. Thanks to the internet, information resources can outweigh natural resources to some extent. An autonomous economy is taking its shape, which is quite often dependent on the efficiency of inter-trust provisioning, not just for subscribers' side, but also for the relying party's side. The federated social operating system leverages legacy identity validation as well as peer-to-peer mutual validation where appropriate, facilitating pervasive trust validation while keeping adequate privacy based on owner's explicit consent. For cross-border business, the difficulties lie in not only the subscribers'

trust validation, but also the trust validation of the relying party; the main reason is that relying party registration is generally isolated in different regions, and therefore the level of interoperability is even lower than on the subscriber side in some scenarios. The Trust Assurance Level evaluation is to be implemented based on the semi-static identity proof, e.g., legacy identity CSPs and RP CSPs issued by the authorities, as well as behaviour-based facts, e.g., Proof of Usage (PoU) and Peer-Validation. (PVs).
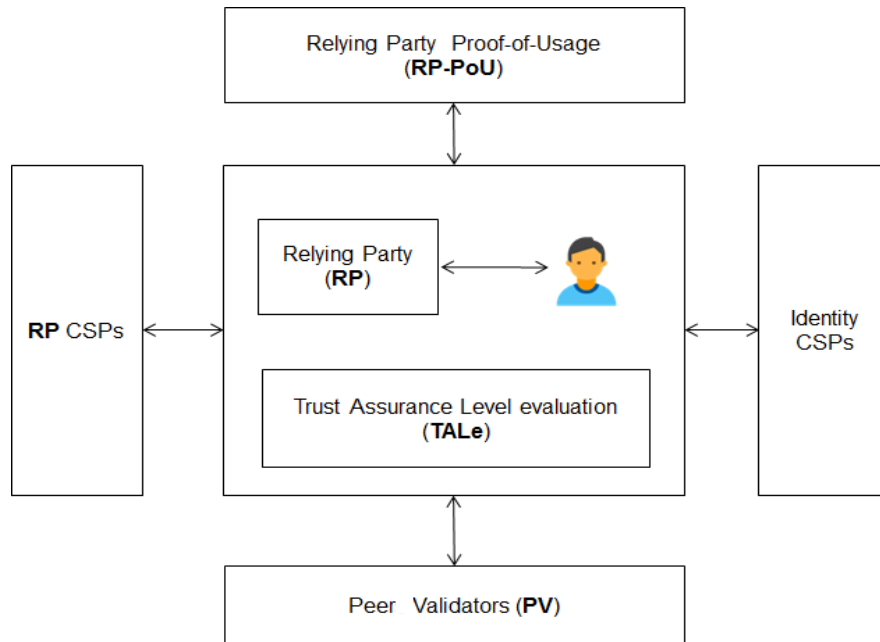
Figure 8: **Future trust framework**

Allowing security stake-holders to engage in open dialogue about the best technologies and tools (including both Open Source and Proprietary technology under protection of SEP/RAND rules) will secure the best possible outcomes in Identity-Proofing Tools (IPT). In the future, exemplar identity-proofing tools for collecting, tagging, aggregating, and fusing digital objects with autonomy at the network endpoints, or groups thereof, will be practical solutions for today's unmet cyber-security, technology, and finance risk dimensions.

7.2   Minimization and data storage scheme for privacy
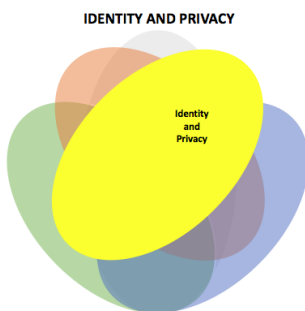
DLT systems will evolve to meet the diverse needs of diverse user communities. This implies that various mechanisms with different strengths -- and weaknesses -- that are fit for particular purposes will be required to interoperate.

7.2.1   Existing best practice techniques

7.2.1.1   Off-chain mechanisms

By introducing "off-chain" mechanisms to store the confidential information separately on another system with access control restrictions and to protect data and manage storage on the DLT, some solutions use only a hash of Personally Identifiable Information (PII), which serves as a reference point and link to an off-chain PII database. Storing information "off-chain" provides privacy of the

transaction details. The "off-chain" system can be set up to restrict access to the transaction details to authorized parties only.

7.2.1.2 Side chains

A "side chain" is a parallel DLT. It sits alongside the primary DLT, serving multiple users and generally persisting permanently. The degree of confidentiality and privacy provided for transactions that take place on side chains depends on what technology the side chain uses.

Additional information can be found in Annex B.

7.2.1.3 Zero-knowledge proofs

Zero-Knowledge Proofs ("ZKP") are a cryptographic technique that enables two parties (a prover and a verifier) to prove that a proposition is true, without revealing any information about that proposition apart from its being true. ZKPs can be used to guarantee that transactions are valid despite the fact that information about the sender, the recipient and other transaction details remain hidden below.

Additional information can be found in Annex B.

7.2.2 Future outlook

Nimble entities with sufficient market power are poised to introduce globally consistent rules for data minimization and use limitation. It is not practical to continue waiting for regulators to act. Multiple examples herald a new age of legal entrepreneurship. A new design construct of Policy Enforcement Points (PEP) is under development that safeguards data owners (a.k.a. transaction authorizers) that are distributed among 11,000 separately governed subnets.

Entities are beginning to interpret over-regulation as damage and are routing around it in an environment characterized by rapidly changing technology, a complex and threatening cybersecurity landscape, and growing competition in an evolving payments ecosystem.

7.2.3 Standardization roadmap

Both off-chain and sidechain mechanisms continue to evolve, and blockchain technology matures. There appears to be little standardization in these areas, and this lack of activity presents opportunities for ITU-T recommendations that could promote interoperable solutions. Given the flexibility provided by ASN.1 encoding can range from verbose XML and JSON formats to the compact binary encodings required by modern telecommunications, standardized ASN.1 schema definition could specify abstract types whose values would be suitable in both the resource rich server environment as well as the constrained environments of smart cards, high volume transaction systems, and the Internet of Things (IoT).

The recent November 2018 outcomes are related to accuracy, fidelity and efficiency of the naming and discovery of digital objects without restricting the use of internet protocols. Doing otherwise risks impeding the evolution of new technologies.

8 Outlook 4: Security and resilience

Quantum-resistance of the cryptographic algorithms underlying DLTs is a must for systems to stand the test of time – whenever those DLTs are meant for use through the next decades and in particular, for critical systems. Likewise, a DLT system should have the ability to resist DDoS and Sybil attacks or dishonest node(s) and in case of failure (of the resistance mechanisms), it should have the ability to revert to its previous known clean state.

8.1 Context stamp

SECURITY AND RESILIENCE

Security and Resilience

With the advent of DLT technologies, it has become possible to securely timestamp information in a decentralized and tamper-proof manner. This implies trust anchors will be used more often in the future.

8.1.1 Existing studies

8.1.1.1 Decentralized time stamp

Data can be hashed and the hash can be incorporated into a transaction stored in the DLT, which serves as a secure proof of the exact time at which that data existed. The proof is due to a tremendous amount of computational effort performed after the hash was submitted to the DLT. Tampering with the timestamp would also lead to breaking the integrity of the entire digital economy, thus it is important to validate the time stamp scheme.

8.1.2 Future outlook

8.1.2.1 Location stamp

An association between time stamp and location stamp may be needed for some special cases. Already technologies such as What3Words.com enable human-friendly naming of every LAT/LONG location on the planet. Other kinds of context stamps may machine-friendly, human-friendly, or both. In supply-chain activities, knowing where and when goods were located in time and space can be identified and stored in a DLT-based repository. This can occur wherever and whenever there is a need. In the future many other contextual attributes may also bind to Time/Location stamps as needed by applications.

8.1.3 Standardization roadmap

In a blockchain implementation, the timestamp on the block data may come from a local system clock or from a calibrated clock maintained by a trusted Time Stamp Authority (TSA). The type of time value used may vary by implementation, but it should be based on documented policy, and meet the requirements agreed to by the participants. In some resource constrained environments, such as the Internet of Things (IoT), a local time value may be the only possibility. Even in resource rich environments, the accuracy demanded by applications can vary as can the requirements for accurate timestamps.

Trusted time stamps can provide greater assurance of the validity of the sequence of blocks. Using time from a TSA ensures that an independent third-party audit can be used to validate the controls used to operate the TSA time stamp process. Unlike locally sourced time that must be continuously synchronized to ensure accuracy among distributed systems, a TSA relies on time sourced from a National Measurement Institute (NMI) or the other master clocks that are upstream from a TSA that

provide calibrated time services. The time source for an NMI is the Bureau International des Poids et Measures (BIPM) near Paris, France, which calibrates the NMI clocks used to calibrate a TSA.

Several existing national and international timestamp standards have been specified by different SDOs. Though they can be considered roughly equivalent for purposes of interoperability, each of these standards specify variations not supported by all of the others. Standards supporting common functionality (e.g., PKI-based timestamps) include ANSI X9.95, ETSI EN 319 421 (replaces TS 101 861), ISO/IEC 18014 (Parts 1-4), and IETF RFC 3161.

When time from a trusted TSA is useful in a blockchain system, industry would benefit from an ITU-T recommendation. An ITU-T recommendation could be based on a profile of the ISO/IEC 18014 standard. At a minimum, such a profile could include only the common functionality supported by the other time stamp standards. The ASN.1 schema specified in ISO/IEC 18014 could be updated and extended to support the new encoding rules of ASN.1 that were not available at the time the ISO/IEC standard was published. Such an extension would include the widely used XML Encoding Rules (XER) and the Octet Encoding Rules (OER) used in the financial services.

8.2 Consensus

SECURITY AND RESILIENCE
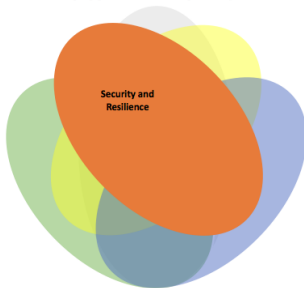
A core technical component of DLT is consensus: how to reach agreement among a group of nodes. Its application to open blockchains has revitalized the field and led to a plethora of new designs, however, the inherent complexity of consensus protocols and their rapid and dramatic evolution makes it hard to contextualize the design landscape. This clause identifies the gap between legacy consensus schemes in application and the practical requirements for the benefits of sustainability, fairness as well as security in adequate performance.

8.2.1 Existing studies

A broad portfolios of consensus schemes have been proposed in the past decades, and it is important to consider the pros and cons of these schemes before the future forecast. Thus, metrics were considered herein for further analysis.

8.2.1.1 Evaluation metrics

Both security and performance are studied in the industry for variants of consensus schemes.

Security metrics

In terms of security, three aspects are considered:
- Consistency – Whether or not the system will reach consensus on a proposed value;
- Transaction censorship resistance – The system's resilience against malicious nodes suppressing transactions;
- DDoS resistance – The system's resilience against DoS attacks against nodes involved in consensus.

Performance metrics

In terms of performance, three aspects are considered:
- Throughput – The maximum rate at which values can be agreed upon by the consensus protocol;
- Scalability – The ability to maintain throughput when consensus involves a larger number of nodes;
- Latency – The time it takes from when a value is proposed until when consensus on it has been reached.

8.2.1.2 Comparative analysis over performance

Based on the above metrics, as a common reference throughout the technical dimension on PoW, PoX, and hybrid consensus, focusing on parts of the table relevant to each category. The wide view captured by Table 4 [b-Bano] aids in visualizing evaluation of the field.

Due to its probabilistic leader election process combined with performance fluctuations in decentralized networks, Bitcoin offers only weak consistency and also leads to excessive energy consumption. To achieve strong consistency and similar performance as mainstream payment processing systems like WechatPay, Visa and PayPal, a number of recent proposals seek to repurpose classical consensus protocols for use in decentralized blockchains [b-Vukolic-a]. The results shown in the table below is sourced from the corresponding references, it shows that since no baseline is defined as of August 2019, the performance of different schemes is variant and not easy to reach consensus in terms of performance.

Table 4: Comparative analysis of consensus schemes

	Systems	Committee Formation (Resources)	Strong Consistency	Single Committee				Multiple Committee			Safety			Performance			
				Committee Configuration	Inter-Committee Consensus			Intra-committee Configuration	Intra Consensus	committee	Transaction Censorship Res.	DoS Res.	Adversary Model	Throughput	Scalable	Latency	Exp. Setup
					Incentives (Join,Participate)	Leader	Msg.		Mediated	Incentives							
Hybrid	ByzCoin [b-Kogias]	PoW	√	Rolling (singl)	√ ×	Internal	O(n)	/	/	/	√	part	33%	1000 tx/s1	×	10–20s 1	Real
	Solidus [b-Abraham]	PoW	√	Rolling (singl)	√ √	External	O(n2)	/	/	/	×	part	33%	/	/	/	/
	Algorand [b-Gilad]	Lottery	√	Full swap	××	Internal	O(n2)	/	/	/	×	√	33%	90 tx/h 2	×	40s 2	Real
	Hyperledger [b-Vukolic-b]	Permissioned	√	Static	/	Flexible	Flexible	/	/	/	√	√	33%	110k tx/s 3	×	<1s 3	Real
	Tencent TrustSQL	Permissioned	√	Static	/	/	/	/	/	/	√	√	50%	50k+tx/s 12	×	20ms 12	Real
	RSCoin [b-Danezis]	Permissioned	√	Static	/	Internal	O(n)	×	Client	×	√	√	33%	2k tx/s 4	√	<1s 4	Real
	Elastico [b-Luu]	PoW	√	Full swap	√ ×	Internal	O(n2)	Dynamic (Random)	!	!	×	√	33%	16 blocks/110s 5	√	110s/ 16 blocks	Real
	Omniledger [b-Kogias-b]	PoW/PoX	√	Rolling (subset)	√ ×	Internal	O(n)	Dynamic (Random)	Client	×	√	√	33%	≈10k tx/s 6	√	≈1s 6	Real
	Chainspace [b-Bassam]	Flexible	√	Flexible	××	Internal	O(n2)	×	×	×	√	part	33%	350 tx/s 7	√	<1s 7	Real
Proof-of-X	Ouroboros [b-Kiayias]	Lottery	×	Full swap	√ √	Internal	O(nc)	/	/	/	×	√	50%	257.6 tx/s 9	×	20s	Simulation
	Praos [b-David]	Stake	×	Rolling (subset)	√ √	Internal	O(1)	/	/	/	×	part	50%	/	/	/	/
	Snow-white [b-Daian]	Stake	×	Full swap	√ √	Internal	O(1)	/	/	/	×	√	50%	100-150 tx/s 9	√	?	Simulation
	PermaCoin [b-Miller]	PoW/PoR11	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	/	×	/	/
	SpaceMint [b-Hønsi]	PoS	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	?	×	600s	Simulation
	Intel PoET [b-Intel]	TH12	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	TH12	1000 tx/s 10	√	/	Real
	REM [b-Zhang]	TH12	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	TH12	!	√	/	Real
Proof-of-work	Bitcoin [b-Nakamoto]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	7 tx/s	×	600s	Real
	Bitcoin-NG [b-Eyal]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	part	50%	7 tx/s	×	<1s	Simulation
	GHOST [b-Sompolinsky-b]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	/	×	/	/
	DECOR+HOP [b-Lerner]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	30 tx/s 8	×	60s	Simulation
	Tencent TrustSQL	PoW	√	Rolling (singl)	× √	Flexible	O(1)	/	/	/	√	√	50%	50k+ tx/s 12	×	50ms	Real
	Spectre [b-Sompolinsky-a]	PoW	×	Rolling (singl)	× √	Internal	O(1)	/	/	/	√	√	50%	/	×	/	/

1 144 nodes/committee.
2 50k nodes/committee.
3 4 nodes/committee (corresponding to BFTSmart [b-Kim]) corresponding to HyperLedger v0.6, new consensus scheme [b-Thakkar] is used after v0.6.
4 3 nodes/committee. 10 committees.
5 100 nodes/committee. 16 committees.
6 72 nodes/committee (12.5% adversary). 25 committees.
7 4 nodes/committee. 15 committees.
8 1 minute average interval; 1 block = 1 MB.
9 40 nodes.
10 As reported in a blog post [b-Kiktenko].
11 proof-of-retrievability
12 16 nodes (corresponding to bft-raft) based on the evaluation results of Trusted Blockchain Alliance (under Ministry of Information Industry of China).

8.2.2 Future outlook

The major hurdles to overcome before widespread adoption of DLT can be realized is their performance, scalability and security. While improvements have been made, they are not at the level of their traditional counterparts. These properties are deeply related to the consensus protocol—the core component of the blockchain. We believe this is where future efforts to improve blockchain performance, scalability and security should be concentrated.

8.2.3 Standardization roadmap

The baseline could be developed for evaluation purpose for different categories of usage context.

Security levels for consensus

The security levels can be defined based on different consensus schemes and the relevant protection profiles. One example is as follows:
- Security level 1: Security level for IOT
- Security level 2: Security level for personal data
- Security level 3: Security level for finance
- Security level 4: Other security level

Environmental impact

Consensus schemes vary significantly in processing power requirements. This affects power consumption and thus their sustainability.

This also presents as one dimension of resilience for sustainability development.

8.3 Resilience of programmability
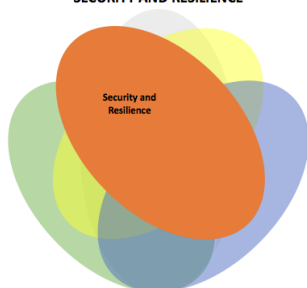
Resilience of programmability is important to guarantee the system resilience, methodologies including formal verification and smart contract test toolkit.

8.3.1 Existing studies

The technique of formal verification has been introduced to improve security by mathematically proving properties about programs. Using formal methods, it is possible to prove that a program is correct for all inputs. The downside is that these are expensive techniques, mostly used in mission-critical software and hardware design.

This technique is especially useful to scripts/smart contracts of DLT systems because these programs are immutable, can store real value and can be accessible publicly from all over the world – in the case of permissionless DLTs. Then, in some cases, the benefits can exceed the high costs.

Some initiatives are being taken to improve the adoption of formal verification in DLT systems.

8.3.1.1 Existing methodologies for secure smart contract scripting
- The process of modelling the design and intended behaviour of a system is proposed in reference [b-Nehai] where rules are derived to translate Solidity smart contracts into NuSMV input language. An alias is defined for each function, the transformation of variables per execution is described, and the conditions and effects of executing external functions (from another contract) are modeled [b-Nehai].

- For more complex smart contracts, the use of ontologies and rules to capture the possibilities and enforce desirable behavior is proposed [b-Nehai]. As ontologies are a representation of information and relationships, they naturally enforce constraints. An individual (object) has properties and relations. The methodology proposed is one that extracts these details from a formal document (clinical trials, financial contracts, etc) either manually or using text analysis, translating the information into an ontology, from which rules can be obtained. Going further, domain specific template contracts are created with predefined constraint variables. These constraint variables would then be searched for in the abstract syntax tree of the script, and automatically updated based on the rules extracted from a document and ontology [b-Nehai].
- The reference [b-Nehai] recognizes the ubiquity of smart contracts as well as the vulnerabilities exacerbated by autonomous environments. In response, the authors propose formal verification, where smart contract code is considered beyond the traditional scripting languages and instead to formal logic. In a two-layer smart contract definition process, the specification logic layer allows for verification and enforcement while the ruler layer defines the implementation details as specified by the former [b-Nehai]. Referencing the DAO attack, such a method allows for the generation of a robust smart contract based on formal specifications of said contract.
- Corda, another decentralized ledger technology platform, proposes to model transactions after real-world scenarios. The platform promises legally enforceable transactions between identifiable parties (unlike un-permissioned blockchains such as Ethereum and Bitcoin) [b-Nehai]. The smart contracts are accompanied by legal proses to which participants can refer during disputes.

8.3.2 Future outlook

8.3.2.1 Insurance associating mechanisms

- There are many accounts of the Bitcoin and Ethereum networks being hacked in recent years. In many cases, hackers took advantage of loopholes within poorly written smart contract code. In the case of the DAO hack [b-Nehai] malicious actors took advantage of code that allowed for a recursively call where Ether can be recovered multiple times before one's balance is updated. Only because a large enough quantity of ethers was taken, did the Ethereum community take notice and act. The hack brought to light the inherent challenges of writing robust smart contracts. The vulnerability was at the application layer, on top of the network. Because they are human written, they are susceptible to errors that can have millions of dollars' worth of consequences. The hack also raised the question of whether actions that are carried out under what is technically and programmatically permissible by the smart contract, including through exploit, is legal.
- Insurance behind transactions is in the hands of developers who write functionality to protect against unexpected behavior in addition to already fault-proof smart contracts. In the case above, a "hard fork" was enacted, splitting the blockchain to recover the lost ethers. In a separate attack, the smart contract of an application running on the Ethereum network was deployed but never initialized. As it was open to all, the first person to initialize it became the owner of the smart contract and thus had enhanced privileges.

8.3.2.2 Turing completeness

Hyperledger Fabric:
- Smart contracts written in general purpose languages (GoLang Node.js, Java) are turing complete and susceptible to DoS and variations of DoS attacks due to looping mechanisms and non-deterministic executions. This risk is compared against the capability to add complex functionalities to applications. As members of a network must be enrolled, having varying levels of trust determined by organizational policy and smart contracts are agreed upon by

stakeholders [b-Nehai], there is a lesser likelihood of non-deterministic behavior and transactions. Hyperledger's ordering system serves as an additional measure that ensures correct order of transactions to avoid forks [b-Nehai]. No system measure exists to address poorly written code.

Ethereum:

- Solidity is (pseudo) turing complete. Vitalik addressed the challenge of loops by introduction gas (fees) for executions. If a malicious actor wishes to execute code that will loop infinitely, there will be a cost. Despite this, Ethereum has experienced several DoS attacks. In 2016, the platform experienced such an attack where transactions made nearly 50,000 operation code executions per block [b-Wilcke], in turn slowing down the network. The gas price per execution was cheap and the attack exploited this vulnerability, as certain actors are willing to pay a small fee to create bottlenecks in the network. Similar to Hyperledger, as a network and really a platform on which developers can deploy their own decentralized applications, the Turing complete nature of Solidity allows for more elaborate and robust applications.

Bitcoin:

- Bitcoin's scripting language lacks looping mechanisms. The simple design decision was to protect Bitcoin from DoS and make transactions deterministic. The technology is contained, where in Turing complete languages, it is not possible to determine if an execution will terminate.

The balance of flexibility and the resilience is of importance to the industry in the near future, efforts spent over improving the capability of flexibility and efforts spent over strengthen the resilience may introduce competition in this domain.

8.3.3   Standardization roadmap

The certification methods for programmability resilience is to be developed in the coming years and the protection profiles could be further verified in different domain based on its usage context.

8.4   Quantum-resistant cryptography in DLT [b-Kiktenko]

Quantum computing and blockchain are two of today's hottest technologies, both linked by cryptography. Blockchain uses cryptography to protect the system, and quantum computing poses a great challenge to traditional cryptography, threatening the security of blockchain systems.

8.4.1   Existing studies

Blockchain is a decentralized, distributed system that uses encryption to protect against tampering and achieve node consensus. The main encryption applications in the blockchain systems include:

- Hash function for PoW calculation.
- Signature and digital signature.
- Verifiable random function (VRF).

Quantum computing breaks the limit of traditional computing by allowing unprecedented parallelization. Currently, commonly used quantum algorithms are mainly based on Simon's algorithm [b-Kiktenko], Shor's algorithm [b-Bäumer] and Grover's algorithm [b-Grover]. Additionally, recent research [b-Chen] shows that both currently standardized hashing algorithms, likewise symmetric ciphers and even multivariate public key cryptosystems, are vulnerable to quantum algebraic attacks, "if their condition number is too small" [b-Grover]. Because of the

imminent threat of quantum computing to traditional cryptography, "post-quantum" cryptography has been proposed.

The following table summarizes the current 'State of Play':

Table 5: Examples of quantum-resistant cryptography schemes

Quantum-resistant cryptography	Schemes	How it works?	Applies to blockchain?	Typical protocol
Quantum key Distribution	-	Establishes a secret key by quantum communication channel.	Yes [b-Kiktenko]	BB84, SARG04 [b-ETSI]
Code-based cryptosystems	Random linear error correction code [b-Sendrier].	Through solving syndrome decoding problem [b-ETSI].	No	BCS13, Stern94 [b-ETSI]
Lattice-based cryptosystems	Difficult problems such as the shortest vector (SVP) on the grid [b-MIT].	Through finding the shortest non-zero vector within the lattice [b-ETSI].	Yes [b-UBC]	DDLL13, PDG14 [b-ETSI]
Hash based cryptosystems	Security design of hash functions [b-Hash].	To use one-time signature schemes based on hash functions [b-ETSI].	Yes [b-QRL]	BDH11 [b-Buchmann], Merkle 79
Multivariate cryptosystems	Difficult design of multivariable equations [b-MQEPK].	By solving multivariable equations [b-ETSI].	No	DPW14, Ding04
zk-STARK	Zero knowledge proof. [b-Luciano]	By replacing through automated protocols human auditors as a means of guaranteeing computational integrity over confidential data [b-Sasson]	Yes	zk-STARK [b-Sasson]

As to the systems affected by Grover's algorithm, namely the symmetric cryptosystems, the issue at hand here is that their key space is divided by two, amounting to make 128-bit keys useless in the "post-quantum" scenario. There is work in progress at ISO SC27 WG2 on the subject and the current status of the working draft for the ISO/IEC 18033 standard (part 1) is that when quantum-resistance is sought, algorithms should also offer at least 128-bit level security, which amounts to having 256-bit keys as a new minimum in this case.

8.4.2 Future outlook

It is expected that SDOs will develop a future-proof DLT ecosystem, taking advantage (and the necessary precautions against) the quantum revolution, through the use of quantum-resistant cryptography and whenever possible, quantum key distribution.

8.4.3 Standardization roadmap

Currently, there is a "post-quantum" competition going on at NIST which has attained round 2, with the goal to make a final selection of asymmetric encryption algorithms that are quantum-resistant. On the side of symmetric encryption algorithms, there is no competition, but there are initiatives to study the need to use bigger keys for 5G at the ITU-T SG17 notably, likewise the aforementioned recent development at ISO SC27 WG2, where 256-bit symmetric keys emerge as the new minimum for quantum resistance. Once the quantum-resistant asymmetric cryptographic primitives are standardized, their integration into DLT will be a priority. Regarding hash-based signatures, which are standardized already by the IETF, this should start now to be on time for the arrival of large-enough quantum computers on the market.

9 Outlook 5: Risk and audit

First there was Fintech, then Regtech, now Supervisory Technology (Suptech) has emerged. Instrumentation to acquire, measure and record business and human behavioral processes in a manner that is efficient and comprehensive can satisfy financial controls and assure adherence to regulations.

9.1 Risk management and audit
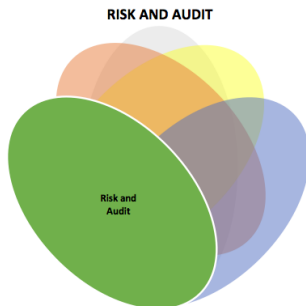
Deployment of DLT in various practical dimensions must fit in where there is need. For example: ITU-T Study Group 17 – Security focuses on security aspects in DLT implying observation and analysis cover the identified risks with existing cases and potential future risks, (e.g., to avoid the replay of Y2K, also the impact of quantum over DLT). Exploration of how to accomplish confidentiality and verified data integrity with minimized resources are important objectives of further study.

9.1.1 Existing studies

Risks are events with a probability that can affect negatively an entity, a process, an organization or an object. Ideally, preventative actions could help to reduce risks, even if some risks have inherent nature.

Auditing is the verification activity to ensure compliance to defined criteria that can be formulated as a standard. Audits have a purpose, which is then defined through a set of appropriate criteria.

Financial audits are, for example, defined against specific standards that are aimed at providing transparencies for investors on the financial results of a company, while security audits are aimed at providing information on how security risks are addressed.

Risk management practitioners are required to understand the environment/business area, to identify relevant risks, measure and monitor them, and design and enforce mitigation activities in line with the risk strategy and appetite.

Some risks have been identified as being of relevance for the whole society and expectations on the preventative and detective activities have been raised by law and regulation. These expectations have been sometime codified as criteria, and audits can be run to identify if the designed and enforced preventative, monitoring and mitigating activities are sufficient.

DLTs are modifying existing risks, introducing as well new risks. The impact on existing risks spans from strategic, commercial, reputational, operational and financial and is caused by changes introduced by new DLT technologies in the existing ecosystems and processes. DLTs are introducing as well new type of risks, mostly related to initially inadequate or incoherent usage of technologies.

9.1.2 Future outlook

9.1.2.1 Auditing and DLT

Audit in relation to DLT could have one of the following dimensions described in the following sections.

Providing assurance on the DLT technologies.

9.1.2.2 Auditing criteria management

The benefits introduced by DLTs in terms of efficiency and trust must not be reduced or limited on one side by the administrative burden to confirm the trust and on the other side need to be confirmed in an interoperable ecosystem.

The criteria defined in the standards, laws and regulations on which auditing is processed nowadays can vary by region. Defining criteria is an on-going process. Some processes can be inter-correlated with each other while others still lack of sufficient cross-check for the uniqueness and coherence, resulting in a waste of resources for potential repetitiveness of auditing, which is neither cost efficient for industry nor for regulatory supervision.

For enhancement, it is necessary to define a mechanism to assist the SDOs to publish sharable criteria that can be applied to the same domain, for example, in figure 9, the SDO1 and SDO2 are belonging to the auditing domain 1, which corresponding to the auditing semantic template set 1; while the SDO3, SDO4 and SDO5 are belonging to the auditing domain 2, which corresponds to the auditing semantic template set 2.
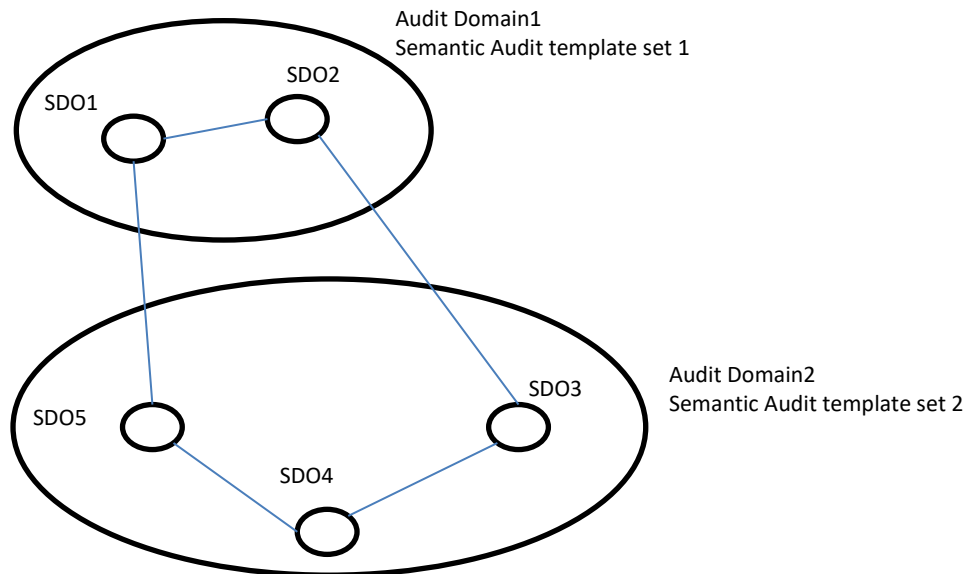
Figure 9: SDOs to publish sharable criteria

The semantic template set is defined in figure 10 as an example, in which the semantic template 1, semantic template 2 and semantic template 3 are pre-defined in one domain, for each semantic template, it can be associated with several metadata and generated from a criteria, each semantic template can be stored in the address corresponding to semantic template digest.

When a SDO publishes new criteria through standards or specifications that can be used in auditing domain 1, a smart contract can be used to compare each new criteria with the corresponding semantic template set, i.e., semantic template 1, including the semantic template 1, semantic template 2, semantic template 3, and so on.

No new criteria is needed to be included in the auditing template set provided the digest of the new criteria are identical with the existing semantic template digest.

In the case that similarity between the legacy semantic template and new criteria is validated, the new criteria digest can be linked to the legacy semantic template digest, thus compiling a complete inter-correlated semantic template for the same set.

In the case that incoherence between the legacy semantic template and new criteria is discovered, the new criteria digest can be linked to the legacy semantic template digest for further potential human justification and decide if a new semantic template is needed for the same set.

The process is to guarantee the uniqueness and coherence of the new criteria in the same domain.
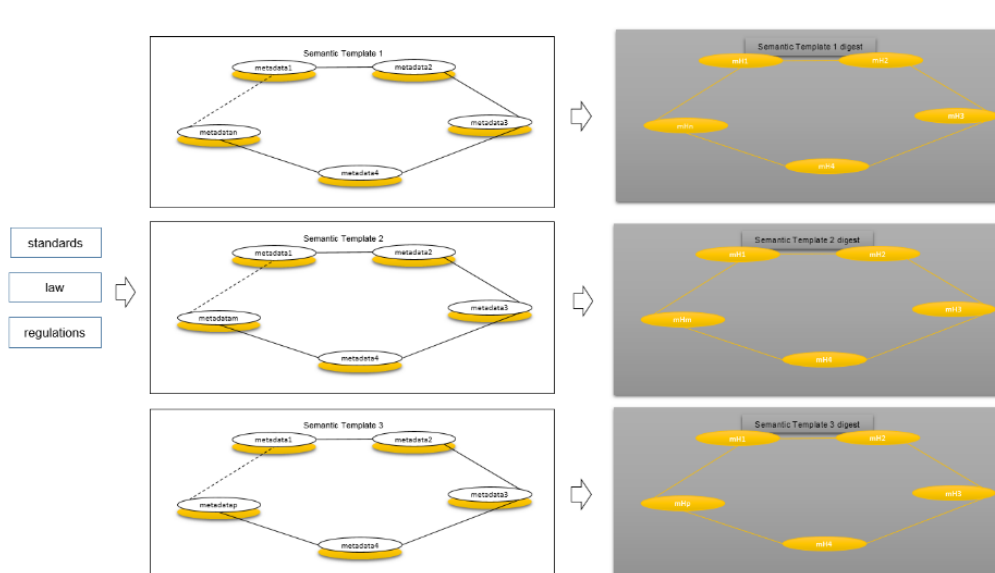
Figure 10: New criteria in the same domain

9.1.2.3 Auditing transactions on the DLT

Auditing transactions on the DLT requires having a copy of the Distributes Ledger and of all related information.

DLT environments have often unique architectures and a lack of standardization. Since organizations have often limited experience on the design of control environment related to DLT based processes and DLTs are designed for real time, with limited access to historical ledger in a form which allows audit, new audit approaches are under development. Audit will become part of the DLT environment. The suggested best practice for obtaining a copy of the Ledger is to have an audit node included in the DLT. This approach would facilitate reporting activities, provide help to assess aspects of the technology built on the DLT and support real time audit solutions.

However, to audit transactions with a node, other elements, in dependency of the use case, need to be considered and addressed. Industry regulation and law may set (independently if the use case is a DLT or not) specific requirements, that need to be auditable on the DLT. The main requirement is that auditing requirements are set on a per use case basis.

Users need to be recognized. The identification of the person may be relevant, i.e. for KYC (refer to the KYC section).

If the use case allows the users remaining anonymous, it may still be important to have consistency of identification along transactions (e.g., if a business control requires to have an approver different from a requestor).

Since information in the transaction may encrypted, the keys to decrypt should be accessible to the auditing function.

Information relevant to the auditing of the transactions may not be contained in the DLT and should be made accessible to the auditing function.

The auditing node should be not authorized to perform transactions. An additional audit monitoring node could be considered.

Independent timestamping could be necessary to address cutoff issues. A real time auditing concept needs to be defined, since there could be use cases where the correct view of the transactions cannot be verified at any point in time, but may be requiring some transitional period, necessary to complete the transaction.

9.1.2.4   Providing assurance on the DLT technologies

DLT are aimed at introducing benefits with trust and efficiency as a value driver. DLT are shifting the trust to the technology. Transactions shift to become irrevocable (principle of non-repudiation) and the integrity of the settlement finality is proven by the DLT. This increases the need to trust the technology. Providing assurance on the DLT technologies requires identifying the purpose of the audit and the corresponding risks and criteria to measure the appropriate dealing of these risks.

The introduction of a new DLT technology-based environment requires to cover new area of risks and more traditional areas with a new mindset.

In particular it, is expected that:
- Roles are designed and enforced as required by regulation;
- An appropriate governance has been put in place, which defines how the DLT solution has to operate, how to identify, monitor and react to risks and how to manage changes and corrections in a decentralized environment;
- Development, tests and deployments take into consideration the specific risk of the DLT technologies, in particular:
  - i)   Direct technological risks: i.e., used keys properties, cryptographic techniques, data structures, sidechains, wallet, consensus mechanisms, etc.;
  - ii) Usage of technologies in the solution: i.e., handling keys/devices, granting and revoking key holders, key backups, wallet management, signing transactions, etc.;
  - iii) Design, approval, testing, and management of smart contracts;
  - iv) Security of the network.

It is also expected by companies embracing a DLT use case to consider the interfaces (physical and processual) between the use case solution and the traditional system world: e.g., how to handle transaction corrections, authorizations.

9.1.2.5   Security aspects

There is a recognized need for unified security and communication functions to authenticate people, protect their messages, and validate their identity attributes, credentials, and authorities over the Internet. Financial Institutions (FIs) and their fiduciary relationships will continue to seek experiences that improve the execution of time-sensitive asset transfers across jurisdictional boundaries.

Digitalization of standard financial instruments such as bonds, fiat currencies, bills of exchange, checks, purchase orders, and payment transfers will continue to accelerate the velocity of funding and collateral. In support of this trend, Real-time Gross Settlement (RTGS) systems are emerging to transfer payments as well as related information of a private and confidential nature such as medical records or other informational assets.

As IoT and other sources of data emerge, the need to protected business processes that release real-time transfer instructions on behalf of Treasury Managers can only execute upon verification that the following conditions apply:

Time-sensitive duties are legally enforceable; bi-lateral information flows are protected by strong access and usage restrictions for the following outcomes beneficial to relying parties:
- Anonymity
- Autonomy
- Atomicity

9.1.2.6   Environmental aspects

Computing is becoming one of the biggest consumers of electric energy [b-Jones]. At the same time, there is an urge to reduce CO_2-emmissions to limit climate change. Disintermediation has the

potential to reduce the energy consumed. Intermediaries have an overhead that is partly paid in terms of energy as well.

DLT in general does not optimize computing efficiency. Peer-to-Peer communication of all contents to every node and redundant storage of content is the least efficient computing model we now. However, creating trust almost always requires additional overhead.

Blockchain should only be used, when specific features of blockchain are required. Then the use of blockchain can offset other processes that would be even less energy efficient.

A special case regarding energy consumption is the proof-of-work consensus algorithm. Bitcoin consumes about 50 TWh/year and Ethereum about 10 TWh/year [b-Digicon]. This is more energy than entire countries like Israel or Greece consume. This energy consumption is related on block rewards, the value of Bitcoin/Ethereum, transaction fees and the price of energy. Therefore, the amount of energy consumed by proof-of-work has been rapidly rising with the rising value of Bitcoin and diminished a bit with fall of the Bitcoin price. The amount of energy used for proof-of-work ensure that a 51% attack is expensive. Reducing the amount of energy used for proof-of-work would be possible but would also reduce the robustness against a 51% attack.

As a defense, it is being said, that any creation of an independent currency is expensive and wasteful. Gold gets dug out of the ground in an energy intensive and toxic process – just to be used as a store of value underground again.

A lot of research focus on better consensus algorithms. An alternative proposed is to replace the current wasteful proof-of-work with a proof-of-work that is solving real mathematical problems. The most common proposition, however, that also Ethereum has started to migrate are variants of proof-of-stake. Most new blockchains do not use proof-of-work.

Whereas blockchain in general can be an environmentally friendly technology when replacing less efficient current systems, it is hard to find an example where the same is true for a blockchain application that uses proof-of-work. Bitcoin has scheduled halving of block-rewards. These halvings will almost reduce the energy consumed by Bitcoin by 50% unless theses halvings are compensated by a rising value of Bitcoin.

A sustainable use of blockchain is possible but cannot rely on proof-of-work. Although the development of new blockchains and the migration of Ethereum to proof of stake are heading in the right direction, it still has to be proven that the use of blockchain will be overall environmentally friendly. When evaluating if a project should use blockchain, the environmental impact should be considered.

9.1.3 Standardization roadmap

DLTs are sources of new risks, but at the same time are introducing benefits with trust and efficiency as a value driver. DLTs are shifting the trust to the technology. Trust in technology is therefore key: Trust criteria for technology need to be designed, enforced and their compliance verified by audits. Since the benefits introduced by DLTs in terms of efficiency and trust must not be reduced or limited by the administrative burden to confirm the trust, it is expected that the different SDOs will develop mechanism to make criteria sharable, coherent and usable in an interoperable ecosystem.

Annex A: Additional information for Outlook 2 – Computational networks

A.1 Programmability and smart contracts: Programmability structure and hierarchy

Smart contracts, written in a multitude of programming languages, are the driving mechanisms within blockchain technologies. Several of today's blockchain frameworks rely on smart contracts to define the underlying business logic. Embedded within the network, these encoded rules govern transactions, ensuring consistent data across the environment.

A.1.1 Hyperledger fabric

- SDKs and APIs are provided for use through client-side applications to invoke the smart contract and interact with the blockchain. Users invoke the functions of the chaincode through these services to make read and write states of assets on the ledger;
- Chaincode (smart contract): Originally written in Golang before scripting capabilities were extended to Node.js and java [b-Hyperledger]. The chaincode consists of functions and object representation of transactions and assets respectively. For this reason, the chaincode is installed on the peer nodes and their respective channels to which they belong. After successful installation, an instantiation transaction is made, initializing the state database with the asset values [b-Ethe-b]. The key functionalities of the chaincode is to put, read, or delete states from the ledger through transactions (history remains) [b-Hyperledger].
- System chaincode: Additional 'chaincodes' can manage and query finer-level system features such as endorsers, block and transaction details. Because of these rudimentary features, the system chaincode is inherent to the peers and is not manually installed like the main client connected chaincode [b-Ethe-b].
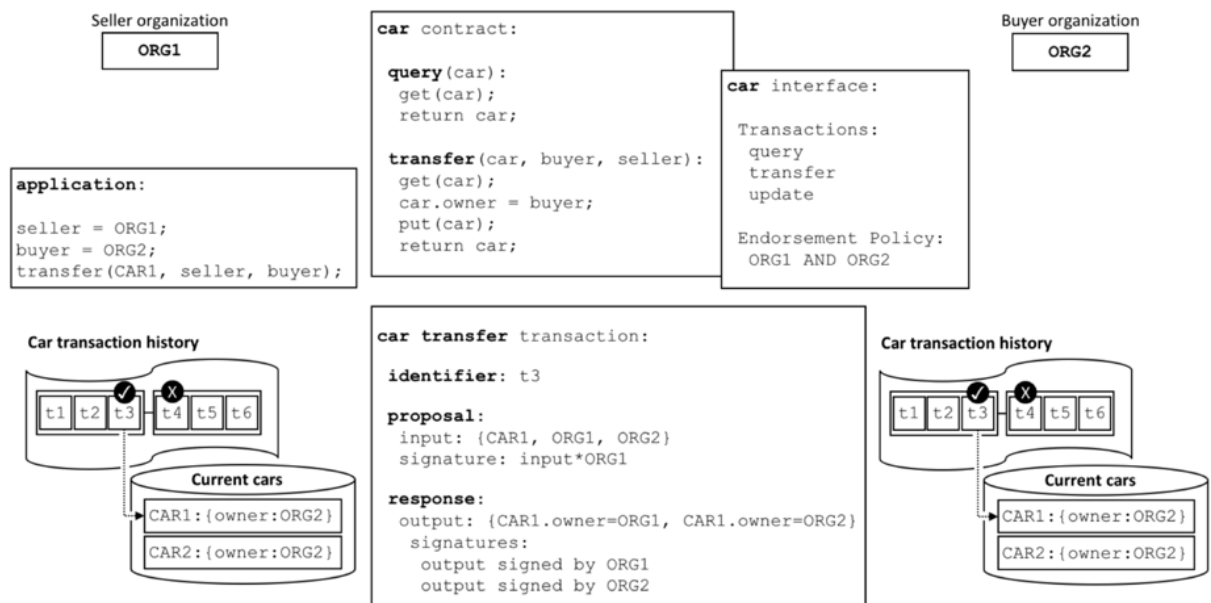
Figure A.1: Hyperledger fabric smart contract components

A.1.2 Ethereum Solidity

- SDKs and APIs: Similar to Hyperledger, the Ethereum platform comprises many APIs and surrounding software to allow developers and general users to interact with applications on the network. Developers can build their own applications, coins (assets), and smart contracts to govern their application [b-Schmid].
- Smart contract: Written in Solidity and stored as bytecode at a specific address on the blockchain. An Application Binary Interface (ABI) provides users insight on how to execute the smart contract's code. Several options are made available for users to run tests. In Remix,

programmers develop, compile, and deploy smart contracts, which they can then to set and retrieve values (amongst other functionalities) from the blockchain. Transactions are manifested in a JavaScript virtual machine within the browser and thus are not saved [b-Klarman]. Ethereum's command line tool Geth enables users to connect to the network and active nodes [b-Lightning]. Here, users can create their own private blockchain, genesis block, and nodes. Of course, this does not affect the main blockchain.

A.2 Dependence management

Dependency management (package management) refers to software tools that enable users to install, update, uninstall programs from their machines with ease. Additionally, package managers maintain a list of the programs and their dependencies to ensure complete installation without missing components.

- Node Package Manager (NPM) is utilized by most blockchain developments - Ethereum, Hyperledger examples:
    - i) Ethereum package manager
    - ii) fabric-client & fabric-fa-client

A.3 Lifecycle management

A.3.1 Hyperledger Fabric

- Install: Peer node administrators enable the installation of the smart contract on peer nodes that will be directly involved in the transaction flow (endorsing).
- Instantiate: The chaincode is instantiated on channel(s) in which peers will invoke the code, the initial ledger values are declared and the endorsing policy for future transactions are set. At this point, the smart contract can be invoked to make updates to asset values. The endorsement policy determines what organizations must execute and sign a transaction for it to be valid [b-Hyperledger]. One instance of a chaincode will operate independently of another instance in a separate channel. Ledger values are channel specific and updated by transactions executed within their respective channel.
- Upgrade: Because chaincodes are channel specific, upgrading a chaincode will only affect the channel in which the upgrade is made.

A.3.2 Ethereum Solidity

- Unlike private blockchains, use of public blockchains entail joining already existing networks, which are open to all for participation. Regular users have little control over the blockchain as they are generated overtimes from transactions and mining. An important detail to note is that while on test networks and blockchains, users can update smart contracts, on the main network that many decentralized applications use, a smart contract cannot be altered once deployed [b-Lightning].

Annex B: Additional information for Outlook 3 – Identity and privacy

B.1 Existing studies – Sidechains

Unlike "off-chain" techniques, which store selected information on a traditional network, but at the expense of the benefits of using a DLT, a "side chain" is a parallel DLT. It sits alongside the primary DLT, serving multiple users and generally persisting permanently. The degree of confidentiality and privacy provided for transactions that take place on side chains depends on what technology the side chain uses.

Side chains are independent. If they fail or are hacked, they will not damage other chains; any damage will be limited within that chain. This has allowed experimentation with pre-release versions of DLT technologies and side chains with different permissions to the primary DLT.

Each side chain network can have a doorman service that enforces rules regarding the information that nodes must provide and the know-your-customer processes that they must complete before being admitted to the network.

In the blockchain model proposed in the Bitcoin paper by Nakamoto, a block is composed of two basic components, a "block of items to be timestamped" and a "block header" [b-Drummond]. The header contains the hash of the block data, and following the first block, a hash-link to the data in the preceding block of the blockchain. Block data and its associated hashes cannot be modified without loss of blockchain integrity.

A sidechain is composed of a set of blocks associated with a block in a parent blockchain. The sets of parent blocks and sidechain blocks are disjoint, sharing no common blocks. The operation of a sidechain is functionally distinct from the operation of its parent. Each sidechain may have characteristics that differ from those of its parent, and from other sidechains.

A sidechain may limit read or write access to a different set of participants than those of its parent. Each sidechain may use its own cryptographic algorithms and security techniques. Each may have a different block size and transaction format, establish its own communications protocol requirements, and select the consensus mechanism used by its sidechain participants.

Sidechains and their parent blockchains can be explicitly associated by including a link to a sidechain block in the block header of a parent block. Associations can be established using a hash-pointer data structure to indicate the location of a block and the hash of its data. An extended hash-pointer can also indicate the data type of the sidechain block being referenced.

An extended hash-pointer data structure allows a block in any type of blockchain, (e.g., R3 Corda, Ethereum, Hyperledger Fabric, etc.), to be identified as a sidechain of a parent blockchain. Sidechains need not be physically collocated with their parents, but can be distributed to other legal jurisdictions and operate in separate security zones. Sidechain blocks may be located on IoT devices or associated with smart phones in FOG environments.

An example abstract schema for an extended hash pointer is defined in the draft ITU-T Study Group 17 draft "X.cms" recommendation as follows:

```
HashPointer ::= SEQUENCE {
   hash        DigestedData  OPTIONAL,
   pointers    Pointers  OPTIONAL
} (ALL EXCEPT ({ -- None present -- }))

Pointers ::= SEQUENCE SIZE(1..MAX) OF pointer Pointer

Pointer ::= CHOICE {
   uri        URI,
   rfid       RFID,
   gps        GPS,
   address    Address,
```

```
   dbRecord  DBRecord,

   ... - Expect other pointer types -
}
```

The independence of sidechains from their parent makes sidechain useful for specialized off-chain processing, experimentation, and prototyping. Sidechains can be permanent or temporary. They can be used to compartmentalize processing activities whose results may be reflected later on the parent blockchain.

A sidechain can be useful in storing temporal information, since the sidechain can be removed without loss of integrity in the parent blockchain. This feature makes it possible to compartmentalize sensitive data, such as PII and to delete the data to comply with right-to-be-forgotten requirements of privacy regulation. In blockchain headers that that are extensible, sidechains can be added or deleted as necessary. This makes them ideal for use in constrained environments by applications that must efficiently manage limited storage capacity.

B.2   Existing studies – Zero-knowledge proofs

A Zero-Knowledge Proof (ZKP) is a cryptographic technique, which allows two parties (a prover and a verifier) to prove that a proposition is true, without revealing any information about that thing apart from it being true. ZKPs can be used to guarantee that transactions are valid despite the fact that information about the sender, the recipient and other transaction details remain hidden [b-Drummond].

A zero-knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARK) is a ZKP that proves some computation fact about data without actually revealing the data. zk-SNARKS are the underlying cryptographic tool used for verifying transactions in Zcash. This is done while still protecting users' privacy.

Interoperable operating rules between separately governed DLTs or between separately governed DLT and one or more separately governed side-chains, requires some knowledge of what is "decryptable" vs "non-decryptable" zero-knowledge proofs. In certain proofs (e.g., zk-SNARKs), even if an attacker is able to compromise the cryptosystem, they will not be able to 'decrypt' the hidden transactions as there is not enough information to recover the original message. The attacker may "fake" proofs however due to probabilistic nature of the prover's Turing-complete computational device. zk-STARKs [b-Werbach] are considered as "non-decryptable" ZK according to this definition, for similar reasons.

B.2.1   Other dimensions of ZK technologies

Some further analysis is as below:

B.2.1.1   Transparency

Is there a trapdoor that, if revealed, allows forgery?

zk-SNARKs require trusted setup, and there exists a forgery trapdoor (if the setup is done correctly, that trapdoor will be hard to find). Do ZKP systems always require a trusted setup phase? zk-STARKs: do NOT require a trusted setup phase, therefore no forgery trapdoor.

B.2.1.2   Double scalability

Nearly-linear proving time and exponentially fast setup + verification time?

zk-SNARKs: nearly-linear proving time *but* setup time is not exponentially fast; only after setup can verifier be exponentially fast (this matters when considering evolving, large scale computations, which   would   require   larger   and   larger   setup   procedures   and   keys). In summation, zk-STARKs achieve double scalability without any setup costs.

B.2.1.3 "Post-quantum" security

When talking about the quantum resistant security of zk-SNARKs and zk-STARKs, the answer is zk-SNARKs-no, zk-STARK-yes.

B.2.2 State-of-play and future considerations pertaining to zero knowledge proofs

In public blockchain networks, all transactions are recorded on the public ledger. Its use as a decentralized public key infrastructure make interactions by storing in an immutable way with clear timestamping to proof the existence and date of creation for decentralized identifiers.

The consequence of transparent sequencing of 'events' is that the whole history of an entity can be traced back by its transactions, once someone's identity is uncovered by a malicious actor. For this reason, interaction specific (pairwise) identifiers are used to avoid correlation.

However, the question remains on whether credentials that are connected to one identifier could be made available to another identifier without the reintroduction of said correlation risk.

One approach to this technical challenge is the use of "Zero Knowledge Proofs". Their use allows two different actors, the "prover" and the "verifier" to exchange the ownership of a piece of data, without actually revealing the data.

The math, probability and cryptography behind ZKP technologies is useful to allow the verifier to prove the ownership of a credential to the verifier, such as a driver's license without revealing the identifier of whichever entity to whom (or to what) has been initially issued. This preservation of confidentiality allays fears that an entity with whom (or with what) one transacts is illegitimate.

Current challenges to the wide application of ZKPs are:

- They can be slow and expensive for proofers to process. While there are many ZKP variants, with a wide range of performance characteristics, they are still to be considered in early stages of development;
- Some identity solutions use ZKPs based on graph isomorphisms and these are exceedingly fast in comparison with other ZKP variants;
- Questions remain on the interoperability of ZKP-based credential exchanges. At this time, standards for a universal applicability of zero knowledge proofs across implementations and technology suppliers do not exist.

B.2.3 Data accessibility

Data may be structured or unstructured. Unstructured data becomes structured via computational process. Protection of data in transit, at rest, and in subsequent process are issues that can affect and be affected by DLT systems. Privacy protection and data usage restrictions for the duration of data lifecycle requires determining the best way to name verified digital objects in a manner that can be accessible (with or without DNS).

This section categorizes naming conventions by entity type to distinguish the interoperability of infrastructure from all data usage perspectives, while associating the legacy context. Aspiration: Identify the key milestones and potential roadmap.

Alongside language and message standards, are Attribute-based Access Control (ABAC) [b-Bouma] and Rule-based Access Control (RBAC) methods to protect data privacy and restrict data usage. Access control models provide a framework and set of boundary conditions upon which the objects, subjects, operations, and rules may be combined to generate and enforce an access control decision.

The objective of ABAC and RBAC 'rules' is to manage the transfer of consequential information in a manner that conveys knowledge of which entity owns the responsibility for the accuracy of verified digital objects.

Data exchanges may occur between side-chain and DLT systems operations with different governance models and/or different constitutional legal systems. To remedy harms caused by a

responsible party's failure to operate data protection and/or access controls properly, a priori agreement which jurisdictional authority will resolve conflict issues is mandatory. Policy Enforcement Point (PEP) signify an intersection of jurisdictional boundaries where data protection and access control duties are clarified.

Entity types of "named" digital objects:
- "Who entities" are natural persons who can act as agents of corporate entities or as individuals;
- "What entities" are objects that may be representations of people, resources, licenses, avatars, sensors, etc., which require the ability to identify them by name and to have these names specify an identity (what is named as defined by connections to attributes);
- "How entities" may be rules, tables, programs, instructions, maps, 'smart contracts'.

Broad-reaching language and messaging standards enable inter-operable exchange of data (including 'named digital objects) across jurisdictional boundaries:
- Universal Business Language standard (ISO 19845);
- Universal Financial Industry Message Scheme (ISO 20022).

"What entities" (e.g., token or account based digital currencies) are the subject of an emergent standard to define how named digital objects at the edge enforce data access behavior across jurisdictional boundaries.
- Security Aspects for Digital Currencies (TS 23526 under SC2) The objective of this technical specification ISO standard is to develop a framework providing attribute-based access control to self-protecting data objects indifferent to network topography or platform.
- Note: TS 23576 for Blockchain and ledger under TC307 is an ISO technical report but not a standard.

"How entities" (e.g., rules, etc.) generally conform to IETF RFC 1958 "Architectural Principles of the Internet" and can work with URLs or DOIs and the content demands.

It is an objective of the FG DLT to leverage, not duplicate, the aforementioned ISO 23526 effort that will eventually lead to a security framework. An envisioned digital security framework that also addresses DLT interoperability requirements can include the capabilities for identity, authentication, and authorization to result in an enveloped security capability.

With this approach, separate modules that can be integrated into selected applications of DLT interoperability. An objective of further research might be to study applications that use blockchains as a medium of exchange in order to understand when intrinsic security is a baseline requirement and when it is not and when additional levels of security extrinsic to these applications are also required.

For example, the ITU focus on blockchain, as a use case for fiat digital currency, has a different emphasis than the upcoming ISO 23526 standard development. Several countries have voiced that the digital currency security ISO standard effort should not include blockchain since it is being emphasized in a separate ISO standard effort.

It is likely that the current ISO blockchain efforts will be cross-referencesd by the ISO digital currency security effort (23526) once the digital currency security effort advances. ISO 23526 authors are working with others in looking at 'cash' and 'cash with applications' to differentiate where anonymity and identity can have roles through security technologies. Perhaps this methodology within a digital currency context can be of use for blockchain since there are similar separations for a closed or open blockchain concept.

Bibliography

[b-Abraham]   Abraham, I., Malkhi, D., Nayak, K., Ren, L., and Spiegelman A. (2016) *Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus.* Available at: https://arxiv.org/abs/1612.02916.

[b-Art. 29 WP]   Article 29 Working Party (2014). Opinion 05/2014 on Anonymization Techniques 0829/14/EN WP 216. Available at: https://www.pdpjournals.com/docs/88197.pdf.

[b-Bano]   Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). *SoK: Consensus in the Age of Blockchain.* Available at: https://arxiv.org/pdf/1711.03936.pdf.

[b-Bassam]   Al-Bassam, M., Sonnino, A., Bano, S., Hrycyszyn, D., & Danezis, G. (2018). *Chainspace: A Sharded Smart Contracts Platform.* In proceedings of the Network and Distributed System Security Symposium (NDSS).

[b-Bäumer]   Bäumer, E., Sobez, J. & Tessarini, S. (2015). *Shor's Algorithm.* Available at: https://qudev.phys.ethz.ch/content/QSIT15/Shors%20Algorithm.pdf.

[b-Bouma]   Bouma, T. (2019). *Self-Sovereign Identity: Shifting the Locus of Control.* Available at: https://medium.com/@trbouma/self-sovereign-identity-shifting-the-locus-of-control-10da1c8757ad.

[b-Buchmann]   Buchmann, J., Dahmen, E., & Huelsing, A. (2011). *XMSS – A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions.* Lecture Notes in Computer Science, Vol. 7071, Post-Quantum Cryptography, DOI 10.1007/978-3-642-25405-5_8.

[b-Chen]   Chen, Y. & Gao, X. (2018). *Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems.* Cryptology ePrint Archive: Report 2018/008. Available at: https://eprint.iacr.org/2018/008.

[b-Choudhury]   Choudhury, O., Rudolph, N., Sylla, I., Fairoza, N & Das, A. (2018) *Auto-Generation of Smart Contracts from Domain-Specific Ontologies and Semantic Rules.* In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).

[b-CNIL]   CNIL (2018). *BLOCKCHAIN - Solutions for a Responsible Use of the Blockchain in the Context of Personal Data.* Available at : https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf. (English version).

[b-CNRI]   CNRI (1997). *Managing Access to Digital Information: An Approach Based on Digital Objects and Stated Operations.* Available at: https://www.cnri.reston.va.us/papers/ManagAccess-1.pdf.

[b-Croman]	Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E. G., Song, D. & Wattenhofer, R. *On Scaling Decentralized Blockchains.* Available at: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf.
[b-Daian]	Daian, P., Pass, R. & Shi, E. (2016). *Snow White: Provably Secure Proofs of Stake.* Cryptology ePrint Archive, Report 2016/919. Available at: http://eprint.iacr.org/2016/919
[b-Danezis]	Danezis, G. & Meiklejohn S. (2016). *Centrally Banked Cryptocurrencies. In Network and Distributed System Security.* The Internet Society.
[b-David]	David, B., Gaˇzi, P., Kiayias, A., & Russell, A. (2017). *Ouroboros Praos: An Adaptively-Secure, Semi-Synchronous Proof-Of-Stake Protocol.* Cryptology ePrint Archive, Report 2017/573. Available at: http://eprint.iacr.org/2017/573
[b-Digicon]	Digiconomist (2019). *Bitcoin Energy Consumption Index.* Available at: https://digiconomist.net/bitcoin-energy-consumption.
[b-DLT-D1.1]	ITU-T Technical Specification FG DLT D1.1 (2019). *DLT Terms and definitions.*
[b-DLT-D1.3]	ITU-T Technical Specification FG DLT D1.3 (2019). *DLT Standardization Landscape.*
[b-DLT-D2.1]	ITU-T Technical Report FG DLT D2.1 (2019). *Distributed Ledger Technology Use Cases.*
[b-DLT-D3.3]	ITU-T Technical Specification FG DLT D3.3 (2019), *Assessment Criteria for DLT Platforms.*
[b-DLT-D4.1]	ITU-T Technical Report FG DLT D4.1 (2019). *DLT Regulatory Framework.*
[b-Drake]	Drake, J. (2018). *Fork Choice Rule for Collation Proposal Mechanisms.* Available at: https://ethresear.ch/t/fork-choice-rule-for-collation-proposal-mechanisms/922
[b-Drummond]	Drummond R., Sporny, M., Longley, D., Allen, C., Grant, R. & Sabadello, M. (2019). *Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes.* W3C. Available at: https://w3c-ccg.github.io/did-spec/
[b-Ergo]	Accord Project (2018). *Ergo Language Guide.* Available at: https://docs.accordproject.org/docs/logic-ergo.html
[b-Ethe-a]	The Ethereum Wiki (2018). *A Next-Generation Smart Contract and Decentralized Application Platform.* Available at: https://github.com/ethereum/wiki/wiki/White-Paper
[b-Ethe-b]	Ethereum (2018) *Ethereum Homestead Documentation.* Available at: http://ethdocs.org/en/latest/network/connecting-to-the-network.html

[b-ETSI]	ETSI (2015). *Quantum Safe Cryptography and Security - An Introduction, Benefits, Enablers And Challenges*. Available at: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
[b-EU Blockchain]	European Blockchain Observatory and Forum (2018). Blockchain and the GDPR. Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_re port_gdpr.pdf
[b-Eyal]	Eyal, I., Gencer, A. E., Sirer E. G. & Van Renesse, R. {2016). *Bitcoin-NG: A Scalable Blockchain Protocol.* In Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation, NSDI'16, pp. 45–59, Berkeley, CA, USA. USENIX Association.
[b-GFSC]	Gibraltar Financial Services Commission (2018). Distributed Ledger Technology (DLT) Regulatory Framework. Available at: http://www.fsc.gi/news/distributed-ledger-technology-dlt-regulatoryframework-270
[b-Gilad]	Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017) *Algorand: Scaling Byzantine Agreements for Cryptocurrencies.* Available at: http://eprint.iacr.org/2017/454.
[b-Grassi]	Grassi, P., Garcia, M. & Fenton, J. (2017). *NIST Special Publication 800-63-3, Digital Identity Guidelines.* Available at: https://pages.nist.gov/800-63-3/sp800-63-3.html
[b-Grover]	Grover, L. K. (1996). *A Fast Quantum Mechanical Algorithm for Database Search.* Available at: https://arxiv.org/abs/quant-ph/9605043
[b-Hash]	*Hash-based Public-key Cryptography.* Post-quantum Cryptography [online]. Available at: https://pqcrypto.org/hash.html
[b-Hønsi]	Hønsi, T. (2017). *SpaceMint: A Cryptocurrency Based on Proofs of Space.* IACR Cryptology ePrint Archive.
[b-Hyperledger]	Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S. W. & Yellick, J. (2018) *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains.* The 13th EuroSys Conference, New York: ACM Press, 2018. https://arxiv.org/pdf/1801.10228.pdf
[b-IMSC]	IMSC PCTF Working Group (2019). *The IMSC Pan-Canadian Trust Framework (PCTF).* Available at: https://drive.google.com/file/d/1P8kFJZfUV7PX25KEkZKk0XftrqqQp9FI/view

[b-Intel]   Intel Corp. (2017). Sawtooth. Available at: https://intelledger.github.io/introduction.html

[b-Jain]   Jain, A, Hong, L. & Pankanti, S. (2000). *Biometric Identification*. Communications of the ACM, Vol. 43, No. 2, pp. 91–98. Available at: https://dl.acm.org/citation.cfm?doid=328236.328110

[b-Jones]   Jones, N. (2018). *How to Stop Data Centres from Gobbling up the Wirld's Electricity.* Nature, Vol 561, No. 7722, pp. 163-166.

[b-Kiayias]   Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2016). *Ouroboros: A Provably Secure Proof-Of-Stake Blockchain Protocol.* Cryptology ePrint Archive, Report 2016/889. Available at: http://eprint.iacr.org/2016/889.

[b-Kiktenko]   Kiktenko, E., O., Pozhar, N., O., Anufriev, M., N., Trushechkin, A., S., Yunusov, R., R., Kurochkin, Y., V., Lvovsky, A., I. & Fedorov, A., K. (2018). *Quantum-secured Blockchain*. Quantum Sci. Technol. Vol. 3, No. 035004.

[b-Kim]   Kim, C. (2018). *Sweden's Land Registry Demos Live Transaction on a Blockchain*. Available at: https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/

[b-Klarman]   Klarman. U., Basu, S., Kuzmanovic, A. & Sirer, E., H (2018). *bloXroute: A Scalable Trustless Blockchain Distribution Network WHITEPAPER*. Available at: https://bloxroute.com/wp-content/uploads/2018/03/bloXroute-whitepaper.pdf

[b-Kogias-a]   Kogias, E. K., Jovanovic, P., Gailly, N., Khoffi I., Gasser, L., & Ford B. (2016). *Enhancing Bitcoin Security and Performance With Strong Consistency Via Collective Signing*. 25th USENIX Security Symposium

[b-Kogias-b]   Kogias, E. K., Jovanovic, P., Gasser, L., Gailly, N., & Ford, B. (2017). *Omniledger: A Secure, Scale-Out, Decentralized Ledger*. Available at: http://eprint.iacr.org/2017/406, 2017

[b-Lerner]   Lerner, S. D. (2015). *DECOR + HOP : A Scalable Blockchain Protocol*.

[b-Liecht]   Ministry for General Government Affairs and Finance (2018) Government Consultation Report on The Creation of A Law on Transaction Systems Based on Trustworthy Technologies (TT) (Blockchain Law; TT-ACT; VTG) and The Amendment of Other Law. Available at: https://nlaw.li/s

[b-Lightning]   Nelaturu K. (2018). *Lightning Network*. Available at: https://medium.com/coinmonks/lightning-network-7fcdf3e7b735

[b-Liquid]   Liquid (2018). *Official Launch of Liquid, a New Crypto Platform Opening Up Liquidity for Crypto Markets Worldwide.* Available at: https://cointelegraph.com/press-releases/official-launch-of-liquid-a-new-crypto-platform-opening-up-liquidity-for-crypto-markets-worldwide

[b-Luciano]	Luciano, A. (2018). *zk-SNARKs — A Realistic Zero-Knowledge Example and Deep Dive.* Available at: https://medium.com/coinmonks/zk-snarks-a-realistic-zero-knowledge-example-and-deep-dive-c5e6eaa7131c
[b-Luu]	Luu, L., Narayananm V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). *A Secure Sharding Protocol for Open Blockchains*. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pages 17–30, New York, NY, USA. ACM.
[b-Lyons]	Lyons, P. (2004). *The End-End Principle and the Definition of Internet.* CNRI Working Group on Internet Governance (WGIG). Available at: https://www.cnri.reston.va.us/papers/Internet-definition-WGIG.pdf
[b-Maloney]	Maloney, C. (2018). *No Coins for You! Beijing Says Security Token Offerings are Illegal.* Available at: https://www.ccn.com/no-coins-for-you-beijing-says-security-token-offerings-are-illegal/
[b-Malta-a]	Malta (2018). Malta Digital Innovation Authority Act ('MDIA'). Available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29 080&l=1
[b-Malta-b]	Malta (2018). The Innovative Technology Arrangements and Services Act ('ITAS Act'). Available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29 078&l=1
[b-Malta-c]	Malta (2018). The Virtual Financial Assets Act ('VFAA'). Available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29 079&l=1
[b-Miller]	Miller, A., Juels, A., Shi, E., Parno, B. & Katz, J. (2014). *Permacoin: Repurposing Bitcoin Work for Data Preservation.* In Security and Privacy (SP), 2014 IEEE Symposium on, pp. 475–490. IEEE.
[b-Mission]	The Mission (2018). *Blockchain Scaling: What is Raiden?* Available at: https://medium.com/the-mission/blockchain-scaling-what-is-raiden-4ba2198048e1
[b-MIT]	MIT [online]. *Lattice-Based Cryptography.* Available at: https://toc.csail.mit.edu/node/197
[b-MQEPK]	*Multivariate-quadratic-equations public-key Cryptography.* Post-quantum Cryptography [online]. Available at: https://pqcrypto.org/mq.html
[b-Nakamoto]	Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Available at: https://bitcoin.org/bitcoin.pdf.
[b-Nehai]	Nehai, Z., Piriou, P. & Frédéric, D. (2018). *Model-Checking of Smart Contracts.* 2018 IEEE Conference on Blockchain. Available at:

https://www.researchgate.net/publication/326753153_Model-Checking_of_Smart_Contracts.

[b-New York]   The New York Convention (1958). Available at: http://www.newyorkconvention.org/.

[b-Open Law]   Open Law. [online] Available at: https://www.openlaw.io/faq.

[b-Orcutt]   Orcutt, M., (2017). *A Mind-Bending Cryptographic Trick Promises To Take Blockchains Mainstream*. MIT Technology Review. Available at: https://www.technologyreview.com/s/609448/a-mind-bending-cryptographic-trick-promises-to-take-blockchains-mainstream/.

[b-Peach]   Peach, L. (2019). *The Internet of Things and the Lightning Network*. Available at: https://medium.com/meetbitfury/the-internet-of-things-and-the-lightning-network-41b93dbb8456

[b-Poon]   Poon, J. & Buterin, V. (2017) *Plasma: Scalable Autonomous Smart Contracts*. Available at: https://plasma.io/plasma.pdf

[b-Preiss]   Preiss, I. (2018). Blockstream's New Liquid Network Asks Us to Rethink Trust. Available at: https://medium.com/chainrift-research/blockstreams-new-liquid-network-asks-us-to-rethink-trust-4d7a7b26860b

[b-QRL]   The Quantum Resistant Ledger [online]. Available at: https://theqrl.org

[b-Rhodes]   Rhodes, D. (2018). *The State of Bitcoin Mining: Legal Regulations Around the World*. Available at: https://coincentral.com/bitcoin-mining-legal-regulations-around-the-world/

[b-Sasson]   Ben-Sasson, E., Bentov, I., Horesh, Y. & Riabzev, M. (2018) *Scalable, Transparent, and Post-quantum Secure Computational Integrity*.

[b-Schmid]   Schmid, D. (2018) *How Do Casper, Plasma and Other Ethereum Upgrades Works?* Available at: https://blog.iqoption.com/en/how-do-casper-plasma-and-other-ethereum-upgrades-works/.

[b-SEC]   SEC (2019). *Initial Coin Offerings (ICOs)*. Available at: https://www.sec.gov/ICO.

[b-Sendrier]   Sendrier, N. (2017). *Code-based Cryptography*. TU Eindhoven. Available at: https://2017.pqcrypto.org/exec/slides/cbctuto-ecrypt.pdf.

[b-Sompolinsky-a]   Sompolinsky, Y., Lewenberg, Y. & Zohar, A. (2016). *Spectre: A Fast and Scalable Cryptocurrency Protocol*. IACR Cryptology Eprint Archive, 2016:1159.

[b-Sompolinsky-b]   Sompolinsky, Y. & Zohar, A. (2013). *Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains*. IACR Cryptology ePrint Archive, pp. 881.

[b-Swiss]   The Swiss Federal Council (2019). *Legal Framework for Distributed Ledger Technology and Blockchain in Switzerland an Overview with a Focus on the Financial Sector.* Available at: https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf.

[b-TCFD]   Task Force on Climate-related Financial Disclosures. [online] Available at: https://www.fsb-tcfd.org/.

[b-Thakkar]   Thakkar, P., Nathan, N. S. & Viswanathan, B. (2018). *Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform.* Available at: https://arxiv.org/pdf/1805.11390.pdf.

[b-Todd]   Todd, R. (2018). *Judge to SEC: You Haven't Shown This ICO Is a Security Offering.* Available at: https://www.law.com/therecorder/2018/11/27/judge-to-sec-this-ico-isnt-a-security-offering/.

[b-UBC]   University of British Columbia [online]. *Quantum-Safe Blockchain.* Available at: https://blockchain.ubc.ca/research/quantum-safe-blockchain

[b-UN-DF]   UN (2019). *United Nations Secretary-General's Task Force on Digital Financing of the Sustainable Development Goals Framework Document.* Available at: https://digitalfinancingtaskforce.org/wp-content/uploads/2019/03/2019-March-FRAMEWORK-DOCUMENT-first-edition-1.pdf

[b-US]   The US Federal Reserve (2019).*Synthetic Identity Fraud in the U.S. Payment System A Review of Causes and Contributing Factors.* Available at: https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

[b-Vukolic-a]   Vukolic, M. (2016). *Eventually Returning to Strong Consistency.* Available at: https://pdfs.semanticscholar.org/a6a1/b70305b27c556aac779fb65429db9c2e1ef2.pdf

[b-Vukolic-b]   Vukolic,M. (2017). *Rethinking Permissioned Blockchains.* In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC '17, pp. 3–7, New York, NY, USA. ACM.

[b-WBGU]   WBGU – German Advisory Council on Global Change (2019). *Digital Momentum for the UN Sustainability Agenda in the 21st Century.* Policy Paper 10. Berlin: WBGU. Available at: https://www.wbgu.de/fileadmin/user_upload/wbgu/publikationen/politikpapiere/pp10_2019/pdf/WBGU_PP10_EN.pdf

[b-WEF]   WEF (2019). The World Economic Forum's Global Risks Report – 2019. Available at: https://www.weforum.org/reports/the-global-risks-report-2019.

[b-Werbach]   Werbach, K. (2018) The Blockchain and the New Architecture of Trust (Information Policy). The MIT Press.

[b-Wilcke]   Wilcke, J. (2016). *The Ethereum Network is Currently Undergoing a DoS Attack.* Available at: https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/.

[b-Zamfir]   Zamfir, V. (2017). *Casper the Friendly Ghost A "Correct-by-Construction" Blockchain Consensus Protocol.* Available at: https://github.com/cbc-casper/cbc-casper-paper.

[b-Zhang]   Zhang, F., Eyal, I., Escriva, R., Juels, A., & Renesse, R. V. (2017). *REM:Resource-efficient Mining for Blockchains.* In 26th USENIX Security Symposium (USENIX Security 17), pp. 1427–1444, Vancouver, BC, USENIX Association.