INTERNATIONAL TELECOMMUNICATION UNION

**TELECOMMUNICATION STANDARDIZATION SECTOR**

STUDY PERIOD 2017-2020

**FOCUS GROUP ON APPLICATION OF DISTRIBUTED LEDGER TECHNOLOGY**

**DLT-O-078**

| | | |
|---|---|---|
| **WG(s):** | WG5 | Geneva, 29 July - 1 August 2019 |

**OUTPUT DOCUMENT**

| | |
|---|---|
| **Source:** | FG DLT Outlook team |
| **Title:** | D5.1 - Outlook on distributed ledger technologies for data access |
| **Purpose:** | Discussion |

| | | | |
|---|---|---|---|
| **Contact:** | Wang Dongyan<br>Tencent<br>China | Email: | alphawwang@tencent.com |

**Keywords:** DLT; blockchain; data access; GDPR; ledger data structure; zero knowledge proof; programmability; consensus; identity; audit; legal perspective; token economy; sustainable development;

**Abstract:** This document contains final text of the ITU-T FG DLT deliverable D5.1 “Outlook on distributed ledger technologies for data access,” for adoption.

International Telecommunication Union

# ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

1 August 2019

ITU-T Focus Group on Application of Distributed Ledger Technology

## Technical Report FG DLT D5.1
## Outlook on distributed ledger technologies
## Release 1

**Summary**
This Focus Group DLT technical report explore trends (e.g., technological, societal) in the field of distributed ledger technologies, which could lead to an evolution (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.

**Change Log**
This document contains Version 1.0 of an ITU-T Technical Report entitled: "*Outlook on distributed ledger technologies for data access*" approved at the ITU-T Study Group meeting held in Geneva, 29 July – 1 August, 2019.

**Disclaimer**
Tokens 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 their technical aspects nor as investments.

**Acknowledgements**

| Title | Name | Given Name | Affiliation | Country | Email |
|---|---|---|---|---|---|
| Mr | Arribas | Ismael | Kunfud | Spain | ismael@kunfud.com |
| Mr | Baumann | Tom | Interactive Leader | Canada | tbaumann@interactiveleader.com |
| Mr | Boldrin | Luca | InfoCert | Italy | luca.boldrin@infocert.it |
| Mr | Cambronero | Giovanni | ANCE, AC | Mexico | giovanni@ance.org.mx |
| Ms | Cram-Martos | Virginia | Triangularity | Switzerland | crammartos@triangularity.net |
| Mr | Davila-Gonzalez | Emilio | European Commission | EU | Emilio.Davila-Gonzalez@ec.europa.eu |
| Mr | Erbguth | Jörn | University of Geneva | Switzerland | joern@erbguth.net |
| Ms | Gao | Yulan | University of Electronic Science and Technology of China | China | yulangaomath@163.com |
| Mr | Griffin | Phillip | Griffin Information Security | USA | phil@phillipgriffin.com |
| Mr | Hochberg | Gal | Clear | Singapore | gal@clearx.io |
| Mr | Karangwa | Jean Paul | National Bank of Rwanda | Rwanda | jpkarangwa@bnr.rw |
| Mr | Kovac | Stiepan | QRCrypto SA | Switzerland | stie@itk.swiss |
| Mr | Li | Michael | Tencent | China | michaelli@tencent.com |
| Ms | Lyons | Patrice | CNRI | USA | palyons@bellatlantic.net |
| Ms | Maranhão | Suzana | BNDES | Brazil | suzana@bndes.gov.br |
| Mr | Mathis | Angelo | PWC | Switzerland | angelo.mathis@ch.pwc.com |
| Mr | O'Brien | Richard | Payment Pathways, Inc. | USA | rick@paymentpathways.com |
| Mr | Payen | Patrice | Symantec | Switzerland | patrice_payen@symantec.com |
| Ms | Reis | Taynaah | Moeda Seeds Bank | Brazil | taynaah@moeda.in |
| Mr | Ruffles | Joseph | Clear | Germany | joseph@clearx.io |
| Dr. | Schenker | Inon | Impact Investments' Innovation | Israel | inon@singularititeam.com |
| Mr | Sylla | Issa | IBM | USA | issa.sylla@ibm.com |
| Ms | Wang | Dongyan | Tencent | China | alphawwang@tencent.com |

| Title | Name | Given Name | Affiliation | Country | Email |
|---|---|---|---|---|---|
| Mr | Xiao | Yue | University of Electronic Science and Technology of China | China | xiaoyue@uestc.edu.cn |
| Mr | Yong | Chao | UESTC | China | yongchaomath@qq.com |
| Prof | Youm | Heung Youl | Soonchunhyang University | Korea | hyyoum@sch.ac.kr |


## Editor:


| | | | | | |
|---|---|---|---|---|---|
| Ms | Wang | “Alpha” Dongyan | Tencent | China | alphawwang@tencent.com |

# CONTENTS

## List of Tables



## List of Figures

# Technical report ITU-T FG DLT D5.1

## Outlook on Distributed Ledger Technologies

*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 any pretention about actually predicting what will happen in the future.*

# 1 Scope

One of the key differences that distinguish human beings from all other creatures on the 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 being 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 over the stones, the bamboos, the clothes and paper, and stored in the libraries from generation to generation. Nevertheless, this history is not complete. Inevitably, precious culture/experience/knowledge was 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.

Distributed Ledger Technology (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.

Outlook on DLT is organized into five thematic groupings: Outlook 1-5. The nature of the Outlook topics sometimes required multiple 'lens' through which the theme could be viewed. Sub-parts follow the structure of: a.) Existing Studies; b.) Future Outlook; and c.) 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 DLT's 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

**Outlook3 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

## 1.1 Background

The mission of this 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

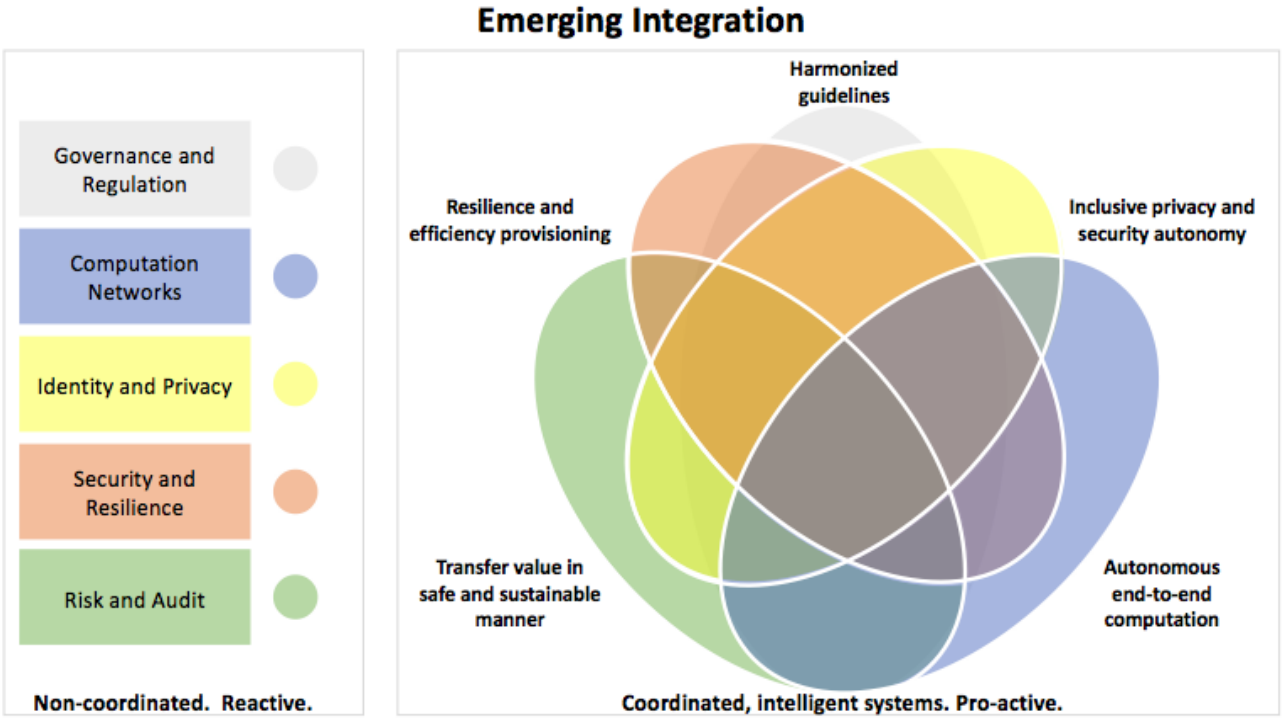



**Figure 1: Surfaces of future considerations for emerging integration**

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 FG-DLT Working Group 3 DLT Platform mapping [3]. ITU FG-DLT Working Group 2 surveyed the DLT landscape [2]. Can we forecast DLT's future and minimize implementation risks upon review of Use Case study by ITU FG-DLT Working Group 3 [3]?

## 1.2 Major objectives

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.


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

It is important to know from whence, how, and why we came to embark on this journey. DLT provides 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 – 2019 [1] 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?

### 1.3 Reference

**[1]** https://www.weforum.org/reports/the-global-risks-report-2019

**[2]** ITU FG-DLT Working Group 2 DLT Use Cases: https://extranet.itu.int/sites/itu-t/focusgroups/fgdlt/_layouts/15/WopiFrame.aspx?sourcedoc={B4654BB9-4CC6-4808-9138-CAAA4746794E}&file=DLT-O-077.docx&action=default

**[3]** ITU FG-DLT Working Group 3 DLT Platform mapping: https://extranet.itu.int/sites/itu-t/focusgroups/fgdlt/input/DLT-I-222.zip

## 2 Terms and definitions

The Technical Report uses the terms defined in FG DLT D1.1: DLT terms and definitions.

## 3 Abbreviations

| | |
|---|---|
| ABAC | Attribute Based Access Control |
| AML | Anti-Money Laundering |
| BFP | Bona Fide Purchaser |
| Client-Server | C/S system |
| CFT | Counter-financing of terrorism or combating the financing of terrorism |
| CSP | Credential Service Provider |
| CNIL | French data protection authority |
| DAG | Directed Acyclic Graph |
| DAO | Digital Autonomous Organizations |
| DaTs | Data Access Technologies |
| DLT | Distributed Ledger Technology |
| DPA | Data Protection Act |
| DPoS | Delegated Proof of Stake |
| ERC | Ethereum Request for Comments |
| 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 |
| IEEE | Institute of Electrical and Electronics Engineers |
| IETF | Internet Engineering Task Force |
| RFC | Request For Comments |
| IOT | Internet of things |

| | |
|---|---|
| ITU | International Telecommunication Union |
| ITU-T | ITU Telecommunication Standardization Sector |
| ITAS Act | Innovative Technology Arrangements and Services Act |
| KYC | Know Your Customer |
| MDIA | Malta Digital Innovation Authority Act |
| PBFT | Practical Byzantine Fault Tolerance |
| PEP | Policy Enforcement Point |
| PIA | Privacy Impact Assessment |
| PII | Personaly Identifiable Information |
| PoA | Proof of Authority |
| PoS | Proof of Stake |
| PoW | Proof of Work |
| RBAC | Rule-based Access Control |
| SDO | Standards Develop Organization |
| STO | Security Token Offerings |
| TrVTs | Trust Value Technologies |
| UNCITRAL | United Nations Commission on International Trade Law |
| UN/CEFACT | United Nations Centre for Trade Facilitation and Electronic Business |
| UTXO | Unspent Transaction Output |
| VFAA | Virtual Financial Assets Act |
| ZK | Zero Knowledge |
| ZKP | Zero Knowledge Proof |
| Zk-SNARK | Zero-knowledge Succinct Non-Interactive Arguments of Knowledge |

# Outlook 1. Governance and 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.*


---

***Part 1. Governance and societal perspectives***

***Part 2. Applicable law and compliance for data assessment***

# Outlook 1. Governance and Legal Regulation

## Part 1. Governance and Societal Perspectives


*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 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.*

### 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's Sustainable Development Goals (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 [1] established by the UN. 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 [2], the Task Force for Climate Related Financial Disclosures (TCFD) [5] and many others, the various initiatives across finance, government, business and civil society 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. In this regard, a recent report, Digital Momentum for the UN Sustainability Agenda in the 21st Century, 2019 [3]recommends 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 INATBA, ConsenSys' Blockchain for Social Impact, and the Climate Chain Coalition.

### 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.

### 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 [4] among others, would help integrate governance innovation with digital innovation to support next-generation sustainability activities.

### 1.4 Reference


**[1]** Task Force on Digital Financing for the SDGs: https://digitalfinancingtaskforce.org/wp-content/uploads/2019/03/2019-March-FRAMEWORK-DOCUMENT-first-edition-1.pdf

**[2]** UN Task Force for Digital Financing: https://digitalfinancingtaskforce.org/

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

**[4]** https://www.openlaw.io/faq

**[5]** Task Force for Financial Disclosures: https://www.fsb-tcfd.org/

# Part 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.*

## 1.1 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.

### 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 WG4. Although the French data protection authority CNIL has voiced its opinion [9] and the Blockchain Observatory at the EU commission has published a summary, [10] 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 [12] 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. Privacy impact assessments (DPIA) are frequently required.

### 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 [8]. The successful injunction in the case of Blockvest BLV tokens [11] does not seem to reverse that rule. China is also taking a strict approach [13]. 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 [4]. Malta has passed three new laws, which introduce certification requirements for ICOs [5], [6], [7]. In Liechtenstein a new law has been passed [14] and Switzerland has published a Federal Council report [Legal framework for distributed

ledger technology and blockchain in Switzerland, Berne 2018-12-14, [15]. Other countries have clarified how existing laws apply to ICOs and STOs.

**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 [3]. New laws on electronic identification and trust services will probably support the use of DLT-based evidence in court.

**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 [1], provider privileges differ among providers: a.) Those that merely do the transmission; b.) 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.

### 1.2 Future outlook

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

**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.

**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.

**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.

**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 coded 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 [2]. 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.

**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.

## 1.3 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, UNECE/CEFACT, UNCITRAL, ETSI, CEN/CENELEC, NIST, DIN, and other communities) are described in more detail in Focus Group DLT Deliverable D1.3 “DLT standardization landscape”.

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

## 1.4 Reference

**[1]** Auto-Generation of Smart Contracts from Domain-Specific Ontologies and Semantic Rules, *2018 IEEE Conference on Blockchain.*

**[2]** New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, http://www.newyorkconvention.org/

**[3]** The State of Bitcoin Mining: Legal Regulations Around the World, Delton Rhodes, Coin Central, 2018-04-08, https://coincentral.com/bitcoin-mining-legal-regulations-around-the-world/

**[4]** Distributed Ledger Technology (DLT) Regulatory Framework, *Gibraltar Financial Services Commission*, 2018-01-02, http://www.fsc.gi/news/distributed-ledger-technology-dlt-regulatory-framework-270

**[5]** Malta Digital Innovation Authority Act ('MDIA'), http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1

**[6]** The Innovative Technology Arrangements and Services Act ('ITAS Act'), http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1

**[7]** The Virtual Financial Assets Act ('VFAA'), http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1

**[8]** Initial Coin Offerings (ICOs), U.S. Securities and Exchange Commission, https://www.sec.gov/ICO

**[9]** Premiers éléments d'analyse de la CNIL: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf english version : https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf

**[10]** European Union Blockchain Observatory and Forum, Blockchain and the GDPR: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf

**[11]** US District Court of Southern California, SEC vs. Blockvest, No. 18CV2287-GPB(BLM), Tod, Judge to SEC: You Haven't Shown This ICO Is a Security Offering, The Recorder, https://www.law.com/therecorder/2018/11/27/judge-to-sec-this-ico-isnt-a-security-offering/

**[12]** Article 29 Working Party (WP29), Opinion 05/2014 on Anonymisation Techniques, 2014-04-10, 0829/14/EN WP216, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

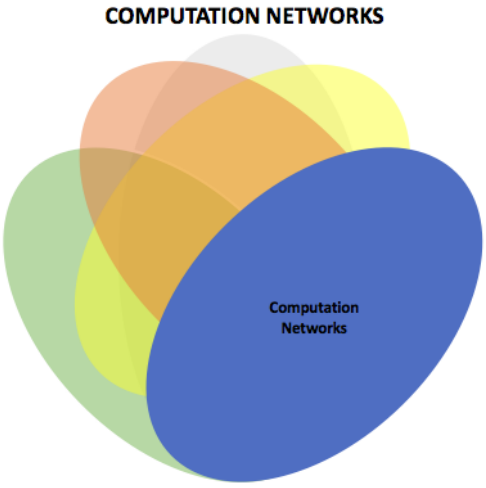
**[13]** CCN, No Coins for You! Beijing Says Security Token Offerings are Illegal, 2018-12-03, https://www.ccn.com/no-coins-for-you-beijing-says-security-token-offerings-are-illegal/

**[14]** https://nlaw.li/1v (an unofficial english translation is available at https://nlaw.li/s)

**[15]** https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf

# 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.*



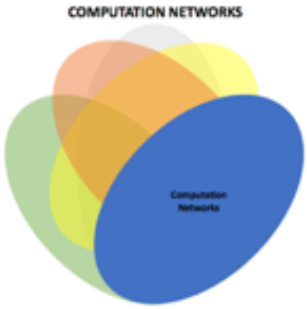

***Part 1. Connectivity capability and high availability***

***Part 2. Programmability and smart contracts***

***Part 3. Ledger data structure***

# Outlook 2. Computation Networks

## Part 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.*

### 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 [1], Ethereum [2], [3], and Hyperledger fabric [4], the typical P2P organization can be categorized into three main types:

a.) Decentralized unstructured topology (e.g., Bitcoin)

b.) Decentralized structured topology (e.g., ETH)

c.) 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 [5]: 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) [9] | ETH [15] | 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 [5] | Layer 2 (off-chain) [10] | ETH [15] | 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 [5] there are several levels of nodes: super full node, top node, single slice node, and light node. | Layer 1 (on-chain) [11] | ETH [15] | Data availability and fraud detection | Partition the existing blockchain into smaller pieces known as shards. |
| **Raiden red ryes** | 1000000 [5]: in the premise of micropayment. | Layer 2 (off-chain) [12] | ETH [5] | Cannot guarantee the security of large transactions. | Off-chain solution for faster and cheaper transactions |
| **Bloxroute** | 200000 [6]: in the premise of that minors run gateway nodes. | Layer 0 [6] | ETH [6] | 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 [7]: in the premise of micropayment. | Layer 2 (off-chain) [13] | BTC [13] | 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 [8] premise: all participants on network accept updates on the network, and no entity can control multiple Liquid Network servers. | Layer 2 (off-chain) [14] | BTC [14] | 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." |

## 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.

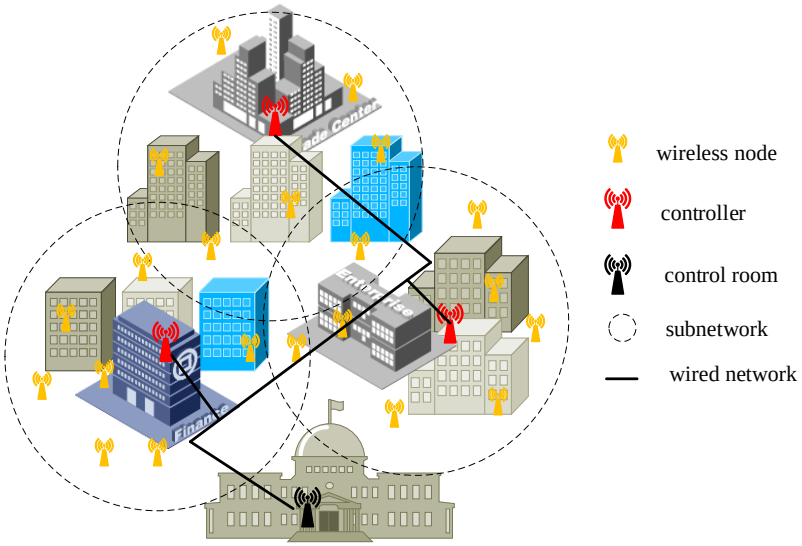



**Figure 3: Hierarchical framework**

As shown in  in the above Figure, 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.

### 1.3 Standardization roadmap

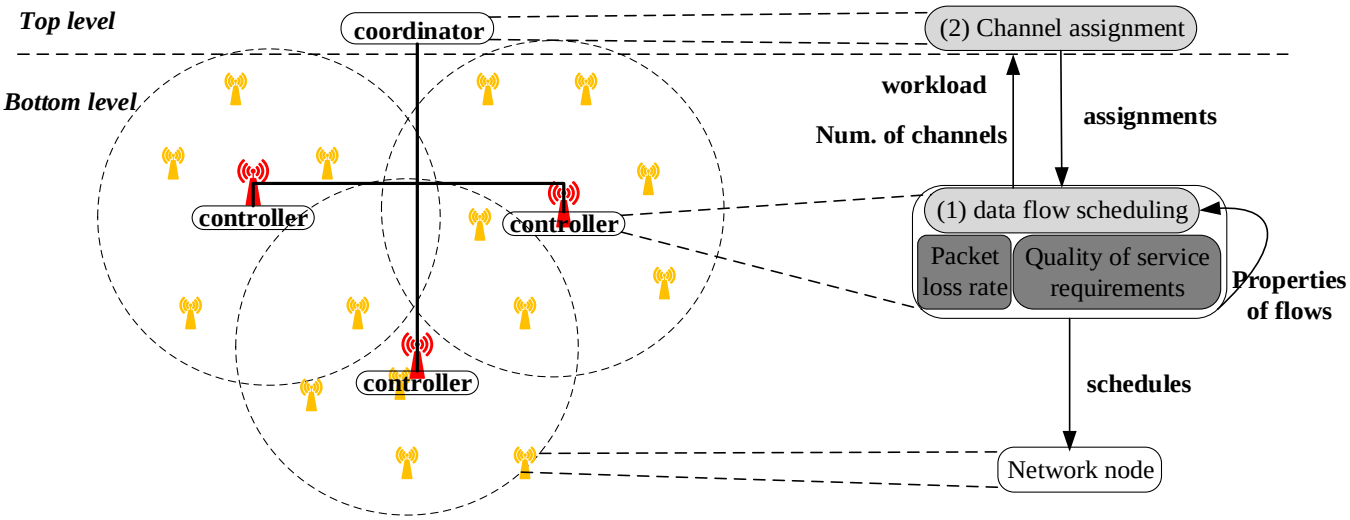



**Figure 4 : Hierarchical management framework overview**

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?

### 1.4 Reference


**[1]** Bitcoin: a peer-to-peer electronic cash system [EB/OL]. (2008-10-31). https://bitcoin.org/bitcoin.pdf

**[2]** Ethereum withe paper. (2018-07-06). https://github.com/ethereum/wiki/wiki/White-Paper.

**[3]** Ethereum homestead documentation. (2018-07-06). http://ethdocs.org/en/latest/network/connecting-to-the-network.html

**[4]** 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

**[5]** https://blog.iqoption.com/en/how-do-casper-plasma-and-other-ethereum-upgrades-works/

**[6]** BloXroute: A Scalable Trustless Blockchain Distribution Network WHITEPAPER

**[7]** https://medium.com/coinmonks/lightning-network-7fcdf3e7b735

**[8]** https://cointelegraph.com/press-releases/official-launch-of-liquid-a-new-crypto-platform-opening-up-liquidity-for-crypto-markets-worldwide

**[9]** Casper the Friendly Ghost A "Correct-by-Construction" Blockchain Consensus Protocol

**[10]** Plasma: Scalable Autonomous Smart Contracts

**[11]** https://ethresear.ch/t/fork-choice-rule-for-collation-proposal-mechanisms/922

**[12]** https://medium.com/the-mission/blockchain-scaling-what-is-raiden-4ba2198048e1

**[13]** https://medium.com/meetbitfury/the-internet-of-things-and-the-lightning-network-41b93dbb8456

**[14]** https://medium.com/chainrift-research/blockstreams-new-liquid-network-asks-us-to-rethink-trust-4d7a7b26860b

**[15]** https://bravenewcoin.com/insights/casper-plasma-and-sharding-a-light-on-ethereums-scaling-spectrum
K. Croman, C. Decker, I. Eyal, et. al., On scaling decentralized blockchains. http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf


## Part 2. Programmability and smart contracts


### 1.1 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.*

**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.

**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: (a) 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. (b) 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 [1].

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.

## 1.2 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. 140

### 1.3 Standardizations 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 [2].

### 1.4 Reference


**[1]** Formal Requirement Enforcement on Smart Contracts Based on Linear Dynamic Logic, *2018 E Conference on Blockchain.*

**[2]** Auto-Generation of Smart Contracts from Domain-Specific Ontologies and Semantic.

**[3]** Model-Checking of Smart Contracts, *2018 IEEE Conference on Blockchain.* https://www.researchgate.net/publication/326753153_Model-Checking_of_Smart_Contracts


## Part 3. Ledger data structure


*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.*

### 1.1 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 Coda 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 8/2019**

| 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) |
| | Multiple hash-chained blocks of | | As required by shard type, most nodes | As required by shard type, only "shards" or | Total for each chain, with "cross-links" to create |

| 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 |
|---|---|---|---|---|---|
| **Sharded / Parachains** | transactions with some relationships | All transactions grow linearly | validate only a subset of all shards. | "chains" participating in transaction | 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 |

## 1.2 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.

## 1.3 Standardization roadmap

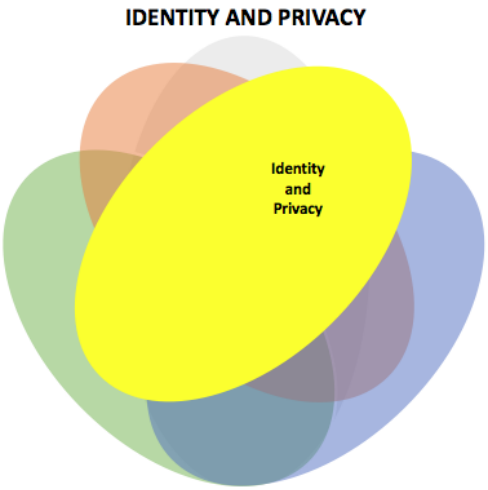
As and when interoperability between chain technologies (and chain instances) becomes a reality, it will happen via some level of standardization – an obvious opportunity for the appropriate standards setting organizations.

## 1.4 Reference

**[1]** S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System," 2008, https://nakamotoinstitute.org/bitcoin/

# 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.*



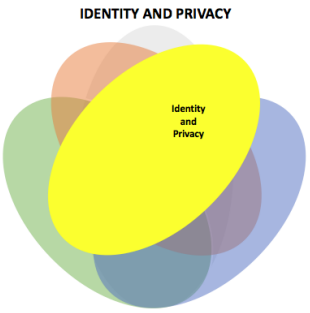

---

***Part 1. Identity and Know Your Customer (KYC)***

***Part 2. Minimization and data storage schemes for privacy***

# Outlook 3. Identity and Privacy

## Part 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.*

### 1.1 Existing studies

Partial list:

- Identity Management Sub-Committee (IMSC) Pan-Canadian Trust Framework [5]
- **eIDAS** (**e**lectronic **ID**entification, **A**uthentication and trust **S**ervices) 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 [6]
- US Federal Reserve Report: Risks of synthetic identity fraud in payments [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.

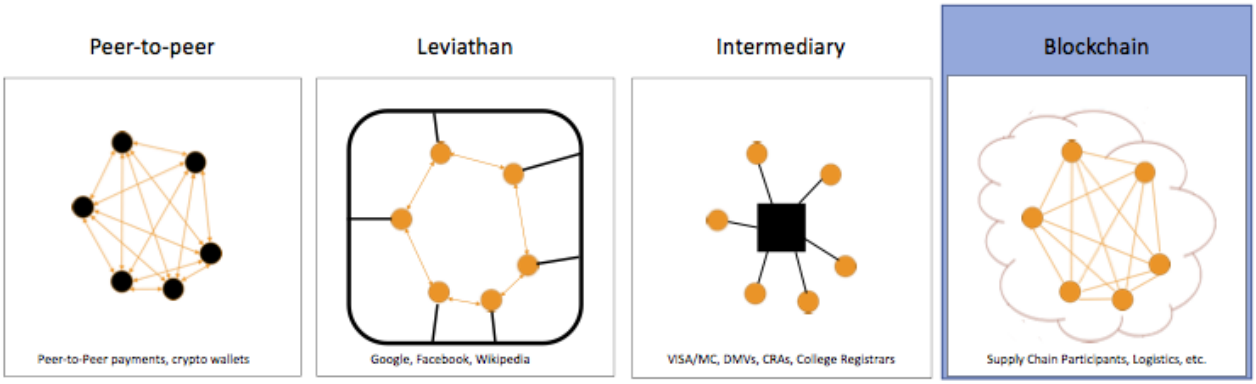



**Figure 5: The trust challenge [2]**

Certain DLT models create a new kind of trust than none of the established models encompass. Subgroup 4 and Subgroup 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: a.) Rules (e.g. for legal enforcement); b.) Identified entities positioned to address challenges; and c.) 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:
    - Within a given centralized signing framework, or
    - 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.

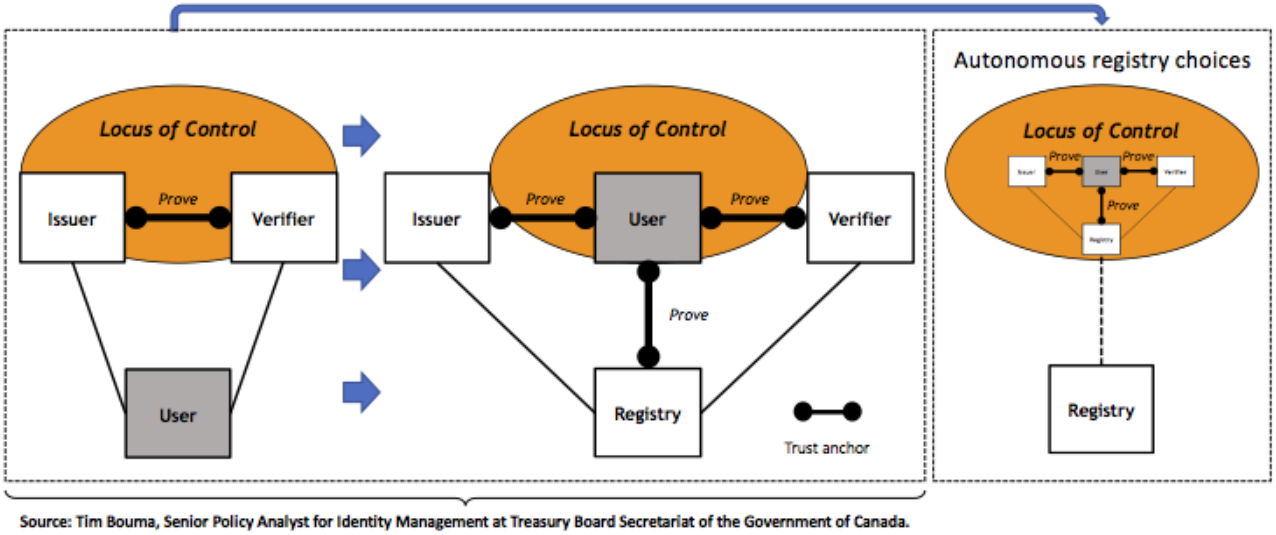



**Figure 6: Locus of power and control [3]**

New computational tools will construct autonomous validity proofs for: a.) A Natural Person's attestation of accuracy for claims that comprise an entity's identifiable characteristics; b.) A Natural Person's intent to activate processes to affect the transfer, storage and retrieval of informational and/or monetary assets; and c.) 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.

**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) [8] [1]. 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.

### 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, eg. 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).

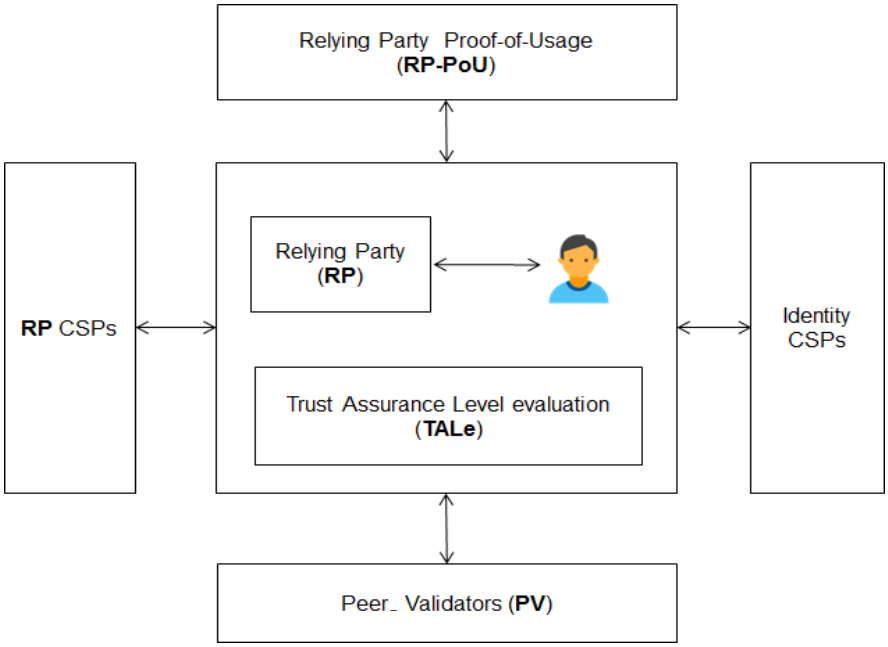



**Figure 7: Future Trust Framework**

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.

### 1.4 Reference

**[1]** Decentralized Identifiers, W3C (https://w3c-ccg.github.io/did-spec/) – Self-sovereign identifiers

**[2]** The Blockchain and the New Architecture of Trust (Information Policy) Kevin Werbach, November 20, 2018, The MIT Press

**[3]** https://medium.com/@trbouma/self-sovereign-identity-shifting-the-locus-of-control-10da1c8757ad

**[4]** https://www.cnri.reston.va.us/papers/Internet-definition-WGIG.pdf

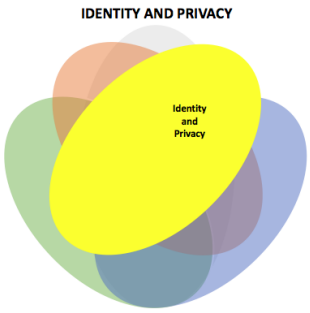
**[5]** Pan-Canadian Trust Framework https://drive.google.com/file/d/1P8kFJZfUV7PX25KEkZKk0XftrqqQp9FI/view

**[6]** https://pages.nist.gov/800-63-3/sp800-63-3.html

**[7]** https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

**[8]** Jain, Hong and Pankanti (2000). Biometric Identification. Communications of the ACM, 43(2), p. 91–98. Retrieved from ACM: https://dl.acm.org/citation.cfm?doid=328236.328110

# Part 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.*

## 1.1 Existing Best Practice Techniques

### 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.

### 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 Annex 2*

### 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 Annex 3*

## 1.2 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.

## 1.3 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.

## 1.4 Reference

**[1]** Orcutt, Mike. "A mind-bending cryptographic trick promises to take blockchains mainstream". *MIT Technology Review*. Retrieved 2018-09-18.

**[2]** Ben-Sasson, et al – Scalable, transparent, and post-quantum secure computational integrity, IACR.org https://eprint.iacr.org/2018/046.pdf - retrieved 2018-09-20

# 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.*


---

***Part 1. Context stamp***

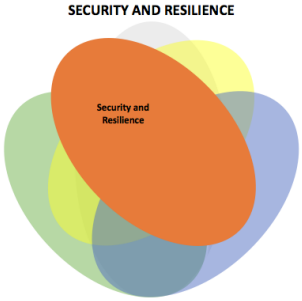
***Part 2. Consensus***

***Part 3. Programmability and smart contracts***

***Part 4. Quantum-resistant cryptography in DLT***

# Outlook 4. Security and Resilience

## Part 1. Context Stamp




*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.*

### 1.2 Existing studies

**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.

### 1.2 Future Outlook

**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.

### 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.

# Part 2. Consensus


*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 section 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.*

## 1.1 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.

### 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

### 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 this table [5] 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 [3]. 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 committee Consensus | | | | | | | | |
| | | | | | Incentives (Join,Par-ticipate) | Leader | Msg. | | Mediated | Incentives | Transaction Censorship Res. | DoS Res. | Adversary Model | Throughput | Scalable | Latency | Exp. Setup |
| Hybrid | ByzCoin[16] | PoW | √ | Rolling (singl) | √ × | Internal | O(n) | / | / | / | √ | part | 33% | 1000 tx/s1 | × | 10–20s 1 | Real |
| | Solidus[6] | PoW | √ | Rolling (singl) | √ √ | External | O(n2) | / | / | / | × | part | 33% | / | / | / | / |
| | Algorand[12] | Lottery | √ | Full swap | ×× | Internal | O(n2) | / | / | / | × | √ | 33% | 90 tx/h 2 | × | 40s 2 | Real |
| | Hyperledger[24] | 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[9] | Permissioned | √ | Static | / | Internal | O(n) | × | Client | × | √ | √ | 33% | 2k tx/s 4 | √ | <1s 4 | Real |
| | Elastico[19] | PoW | √ | Full swap | √ × | Internal | O(n2) | Dynamic (Random) | ! | ! | × | √ | 33% | 16 blocks/110s 5 | √ | 110s/ 16 blocks | Real |
| | Omniledger[17] | PoW/PoX | √ | Rolling (subset) | √ × | Internal | O(n) | Dynamic (Random) | Client | × | √ | √ | 33% | ≈10k tx/s 6 | √ | ≈1s 6 | Real |
| | Chainspace[7] | Flexible | √ | Flexible | ×× | Internal | O(n2) | × | × | × | √ | part | 33% | 350 tx/s 7 | √ | <1s 7 | Real |
| Proof-of-X | Ouroboros[15] | Lottery | × | Full swap | √ √ | Internal | O(nc) | / | / | / | × | √ | 50% | 257.6 tx/s 9 | × | 20s | Simulation |
| | Praos[10] | Stake | × | Rolling (subset) | √ √ | Internal | O(1) | / | / | / | × | part | 50% | / | / | / | / |
| | Snow-white[8] | Stake | × | Full swap | √ √ | Internal | O(1) | / | / | / | × | √ | 50% | 100-150 tx/s 9 | √ | ? | Simulation |
| | PermaCoin[20] | PoW/PoR11 | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | √ | 50% | / | × | / | / |
| | SpaceMint[13] | PoS | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | √ | 50% | ? | × | 600s | Simulation |
| | Intel PoET[14] | TH12 | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | √ | TH12 | 1000 tx/s 10 | √ | / | Real |
| | REM[25] | TH12 | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | √ | TH12 | ! | √ | / | Real |
| Proof-of-work | Bitcoin[21] | PoW | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | √ | 50% | 7 tx/s | × | 600s | Real |
| | Bitcoin-NG[11] | PoW | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | part | 50% | 7 tx/s | × | <1s | Simulation |
| | GHOST[23] | PoW | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | √ | 50% | / | × | / | / |
| | DECOR+HOP[18] | 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[22] | PoW | × | Rolling (singl) | × √ | Internal | O(1) | / | / | / | √ | √ | 50% | / | × | / | / |

1 144 nodes/committee.
2 50k nodes/committee.
3 4 nodes/committee (corresponding to BFTSmart [2]) corresponding to HyperLedger v0.6, new consensus scheme [4] 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 [1].
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).

## 1.2 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.

## 1.3 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.

## 1.4 Reference


**[1]** Crypto Regulation: What's on the G20 Table, Cryptonews 2018-03-04, https://cryptonews.com/exclusives/crypto-regulation-what-s-on-the-g20-table-1325.htm

**[2]** Sweden's Land Registry Demos Live Transaction on a Blockchain, Christine Kim, coindesk, 2018-06-15, https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain/

**[3]** M. Vukolic. Eventually returning to strong consistency. https://pdfs.semanticscholar.org/a6a1/b70305b27c556aac779fb65429db9c2e1ef2.pdf

**[4]** Parth Thakkar, Senthil Nathan N, Balaji Viswanathan, IBM: Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform https://arxiv.org/pdf/1805.11390.pdf.

**[5]** Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis, University College London, United Kingdom 2The Alan Turing Institute Sok: Consensus in the age of blockchain, https://arxiv.org/pdf/1711.03936.pdf.

**[6]** I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman.Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus. https://arxiv.org/abs/1612.02916, Dec 2016. Accessed: 2017-02-06.

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

**[8]** P. Daian, R. Pass, and E. Shi. Snow white: Provably secure proofs of stake. Cryptology ePrint Archive, Report 2016/919, 2016. http://eprint.iacr.org/2016/919.

**[9]** G. Danezis and S. Meiklejohn. Centrally banked cryptocurrencies. In Network and Distributed System Security. The Internet Society, 2016.

**[10]** B. David, P. Gaˇzi, A. Kiayias, and A. Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake protocol. Cryptology ePrint Archive, Report 2017/573, 2017. http://eprint.iacr.org/2017/573.

**[11]** I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse. Bitcoin-NG: A Scalable Blockchain Protocol. In Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation, NSDI'16, pages 45–59, Berkeley, CA, USA, 2016. USENIX Association.

**[12]** Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. http://eprint.iacr.org/2017/454, 2017.

**[13]** T. Hønsi. SpaceMint: A Cryptocurrency Based on Proofs of Space. IACR Cryptology ePrint Archive, 2017.

**[14]** Hyperledger. Sawtooth. https://intelledger.github.io/introduction.html.

**[15]** A. Kiayias, A. Russell, B. David, and R. Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. Cryptology ePrint Archive, Report 2016/889, 2016. http://eprint.iacr.org/2016/889.

**[16]** E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford. Enhancing bitcoin security and performance with strong consistency via collective signing.

**[17]** E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford. Omniledger: A secure, scale-out, decentralized ledger. http://eprint.iacr.org/2017/406, 2017.

**[18]** S. D. Lerner. Decor+ hop: A scalable blockchain protocol.

**[19]** L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena. 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, 2016. ACM.

**[20]** A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz. Permacoin: Repurposing bitcoin work for data preservation. In Security and Privacy (SP), 2014 IEEE Symposium on, pages 475–490. IEEE, 2014.

**[21]** S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, Dec 2008. Accessed: 2015-07-01.

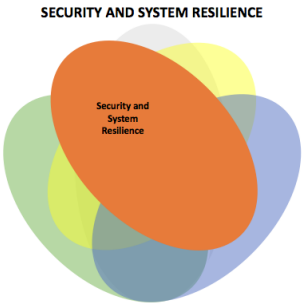
**[22]** Y. Sompolinsky, Y. Lewenberg, and A. Zohar. Spectre: A fast and scalable cryptocurrency protocol. IACR Cryptology ePrint Archive,2016:1159, 2016.

**[23]** Y. Sompolinsky and A. Zohar. Accelerating bitcoin's transaction processing. fast money grows on trees, not chains. IACR Cryptology ePrint Archive, 2013(881), 2013.

**[24]** M. Vukoli´c. Rethinking permissioned blockchains. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts,BCC '17, pages 3–7, New York, NY, USA, 2017. ACM.

**[25]** F. Zhang, I. Eyal, R. Escriva, A. Juels, and R. V. Renesse. REM:Resource-efficient mining for blockchains. In 26th USENIX SecuritySymposium (USENIX Security 17), pages 1427–1444, Vancouver, BC,2017. USENIX Association.

# Part 3 Programmability and smart contracts




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

## 1.1 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 (1) are immutable, (2) can store real value (3) 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.

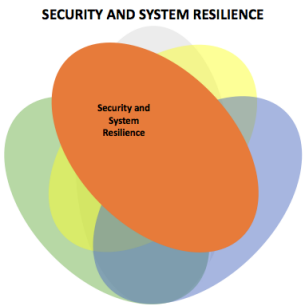
## 1.2 Future outlook

**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.**

## 1.3 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.

# Part 4. Quantum [11]-resistant cryptography in DLT




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

## 1.1 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 system 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[1], Shor's algorithm [2] and Grover's algorithm [3]. Additionally, recent research 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." Because of the imminent threat of quantum computing to traditional cryptography, post-quantum cryptography has been proposed[4].

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 [11] | BB84, SARG04 [5] |
| **Code-based cryptosystems** | Random linear error correction code. [6] | Through solving syndrome decoding problem. [5] | No | BCS13, Stern94 [5] |
| **Lattice-based cryptosystems** | Difficult problems such as the shortest vector (SVP) on the grid. [7] | Through finding the shortest non-zero vector within the lattice. [5] | Yes [12] | DDLL13, PDG14 [5] |
| **Hash based cryptosystems** | Security design of hash functions. [8] | To use one-time signature schemes based on hash functions. [5] | Yes [15] | BDH11 [13], Merkle 79 |
| **Multivariate cryptosystems** | Difficult design of multivariable equations. [9] | By solving multivariable equations. [5] | No | DPW14, Ding04 |
| **ZK-STARK** | zero knowledge proof. [10] | By replacing through automated protocols human auditors as a means of guaranteeing computational integrity over confidential data [14] | Yes | ZK-STARK [14] |

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.

### 1.2 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.

### 1.3 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.

## 1.4 Reference


**[1]** https://www.cnri.reston.va.us/papers/Internet-definition-WGIG.pdf

**[2]** https://qudev.phys.ethz.ch/content/QSIT15/Shors%20Algorithm.pdf

**[3]** https://arxiv.org/abs/quant-ph/9605043

**[4]** https://eprint.iacr.org/2018/008 from Gao et al.

**[5]** 'Quantum Safe Cryptography and Security-An introduction, benefits, enablers and challenges' ETSI White Paper, ISBN No. 979-10-92620-03-0.

**[6]** https://2017.pqcrypto.org/exec/slides/cbctuto-ecrypt.pdf

**[7]** https://toc.csail.mit.edu/node/197

**[8]** https://pqcrypto.org/hash.html

**[9]** https://pqcrypto.org/mq.html

**[10]** https://medium.com/coinmonks/zk-snarks-a-realistic-zero-knowledge-example-and-deep-dive-c5e6eaa7131c

**[11]** Quantum-secured blockchain, E.O. Kiktenko et al., Quantum Sci. Technol. 3, 035004, 2018

**[12]** https://blockchain.ubc.ca/research/quantum-safe-blockchain

**[13]** Buchmann, J., Dahmen, E., and A. Huelsing, "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, 2011.

**[14]** Scalable, transparent, and post-quantum secure computational integrity, Eli Ben-Sasson et al.k IACR e-print 2018/046, 2018

**[15]** https://theqrl.org

# Outlook 5. Risk and Audit

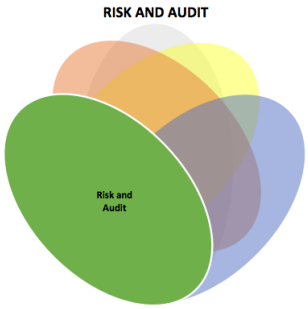
*First there was Fintech, then Regtech, now Supervisory Technology (Suptech) has emerged. Instrumentation to acquire, measure, and record, business and human behavioral processes, in a manner that is efficient and comprehensive, can satisfy financial controls and assure adherence to regulations.*


---

## *Part 1. Risk management and audit*

# Outlook 5. Risk and Audit

## Part 1. Risk management and audit




*Deployment of DLT in various practical dimensions must fit in where there is need. For example: ITU-T SG17 – Security focuses on security aspects in DLT implying observation and analysis cover the identified risks with existing cases and potentia0l 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.*

### 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.

### 1.2 Future Outlook

#### Auditing and DLT

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

#### 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 the figure below, the SDO1 and SDO2 are belonging to the Auditing domain 1, which corresponding to the Auditing Semantic Template Set1; while the SDO3, SDO4 and SDO5 are belonging to the Auditing domain 2, which corresponds to the Auditing Semantic Template Set2.

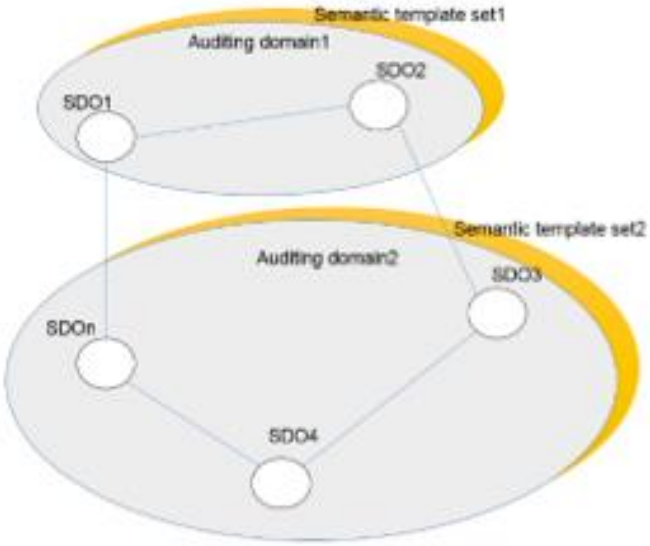



**Figure 8: SDOs to publish sharable criteria**

The semantic template set is defined in the figure below as an example, in which the semantic template1, 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 Set1, including the semantic template1, semantic template2, semantic template3, 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.

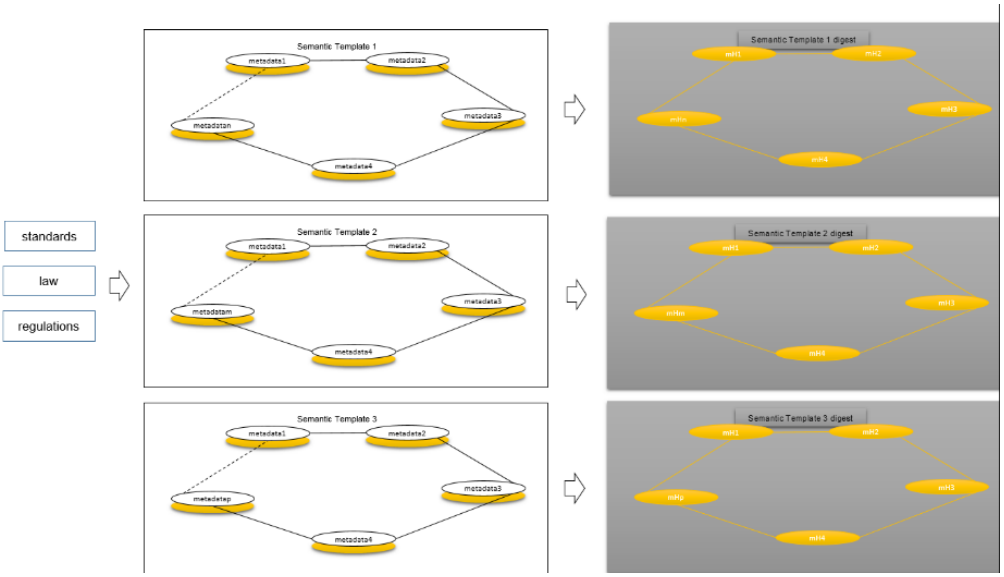



**Figure 9: New criteria in the same domain**

### 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, ie. 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.

**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:
    - Direct technological risks: i.e., used keys properties, cryptographic techniques, data structures, sidechains, wallet, consensus mechanisms, etc.
    - Usage of technologies in the solution: i.e., handling keys/devices, granting and revoking keyholders, key backups, wallet management, signing transactions, etc.
    - Design, approval, testing, and management of smart contracts
    - 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.

**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:

i. Anonymity
ii. Autonomy
iii. Atomicity

**Environmental aspects**

Computing is becoming one of the biggest consumers of electric energy. [1] 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. [2] 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.

## 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.

## 1.4 Reference

**[1]** Nicolas Jones, The Information Factories, nature 2018 p. 163

**[2]** The Digiconomist: https://digiconomist.net/bitcoin-energy-consumption
**[3]** Model-Checking of Smart Contracts, *2018 IEEE Conference on Blockchain.* https://www.researchgate.net/publication/326753153_Model-Checking_of_Smart_Contracts
**[4]** Orcutt, Mike. "A mind-bending cryptographic trick promises to take blockchains mainstream". *MIT Technology Review*. Retrieved 2018-09-18.
**[5]** S. Nakamoto, "Bitcoin: A Peer-To-Peer Electronic Cash System," 2008, https://nakamotoinstitute.org/bitcoin/
**[6]** Ben-Sasson, et al – Scalable, transparent, and post-quantum secure computational integrity, IACR.org https://eprint.iacr.org/2018/046.pdf - retrieved 2018-09-20

# Annex 1

Additional info for Outlook2 computational network part 2 cont

**Programmability and Smart Contracts**

**1.2 Future Outlook – additional notes**

**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.

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 Nodejs and java. [3]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. [3]The key functionalities of the chaincode is to put, read, or delete states from the ledger through transactions (history remains). [3]
- 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. [3]

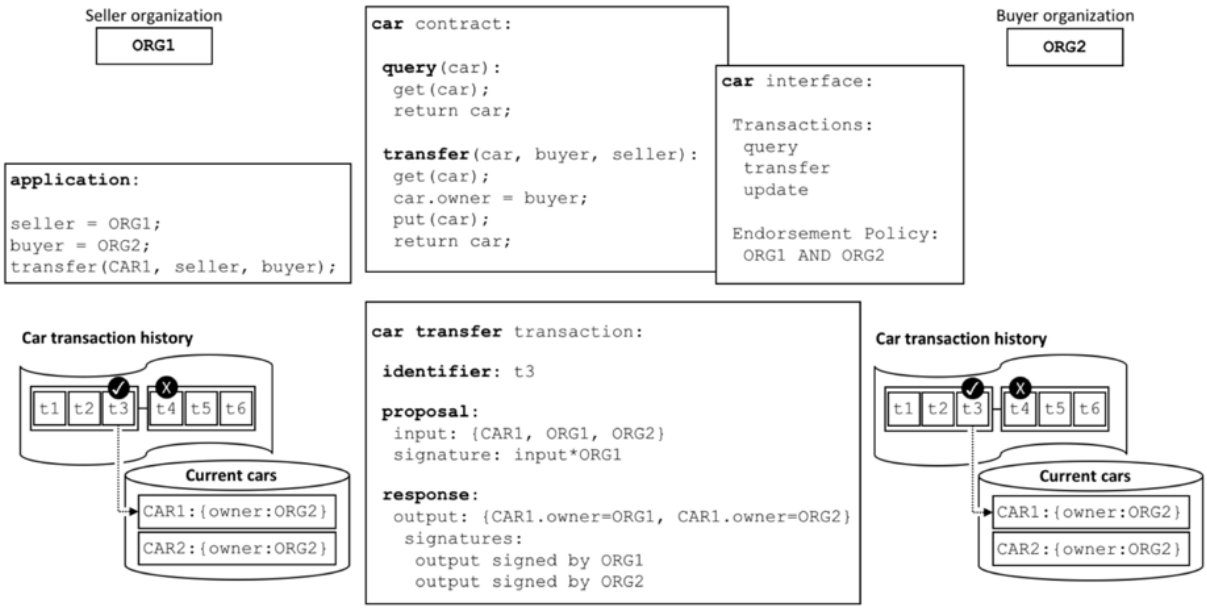



**Figure 10: Hyperledger Fabric Smart Contract components**

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. [3]

- Smart contract: Written in Solidity and stored as bytecode at a specific address on the blockchain. An ABI (Application Binary Interface) 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. [3] Ethereum's command line tool Geth enables users to connect to the network and active nodes. [3]Here, users can create their own private blockchain, genesis block, and nodes. Of course, this does not affect the main blockchain.

**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

**Lifecycle management**

Hyperledger:

- 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. [3]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.

Ethereum:

- 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. [3]

**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 [3]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.

**Turing Completeness**

Hyperledger Fabric:

- Smart contracts written in general purpose languages (GOLANG, NodeJS, 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, [3] 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 [3]. 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, 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.

**Existing methodologies for secure smart contract scripting**

- The process of modelling the design and intended behaviour of a system is proposed in reference [3]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. [3]
- For more complex smart contracts, the use of ontologies and rules to capture the possibilities and enforce desirable behavior is proposed. [3] 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. [3]

- The reference [3]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. [3]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). [3]The smart contracts are accompanied by legal proses to which participants can refer during disputes.

# Annex 2
# Additional info for Outlook3 Identity and Privacy

### 1.1 Existing Studies – Sidechains – additional notes

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 won’t 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.” [1]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 personally identifiable information (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.

# Annex 3

# Additional info for Outlook3 Identity and Privacy

## 1.1 Existing Studies – additional notes

### Zero-knowledge proofs – additional notes

#### Overview

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. [1]

A Zk-SNARK (Zero-knowledge Succinct Non-Interactive Arguments of Knowledge) 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 [2] are considered as "non-decryptable" ZK according to this definition, for similar reasons.

#### Other dimensions of ZK technologies

Some further analysis is as below:

#### 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. This is clear and understood upfront.
Transparently, there is no trusted setup, no forgery trapdoor.

#### 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.

#### Post-quantum security

Comments from Eli believes that Zk-SNARKs can not survive in post-quatum era; while Zk-STARKs take some advantage in post-quantum era. However, the next version of the X.509 recommendation proposed a hybrid signature certificate extension that allows the security risk to digital signatures of post quantum computing (PQC) to be managed. The proposed extension allows certificate and certificate revocation list (CRL) content to be doubly signed, once with an existing signature algorithm and then a PQC resiliant algorithm.

#### 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;
  and
- 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.

**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) 错误!未找到引用源。 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-referenced 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.