International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Technical Report

(1 AUG 2019)

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

Technical Report FG DLT D4.1

Distributed ledger technology regulatory framework

FOREWORD

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

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

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

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

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

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

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

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

© ITU 2019

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Technical Report FG DLT D4.1

Distributed ledger technology regulatory framework

Summary

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

It considers the key properties of distributed ledger technology (DLT) that are common among the diverse approaches. It brings into focus the topics that are of concern to regulators and supplies practical recommendations for users, regulators, and technologists, we hope to mitigate the risks of potential harms.

Keywords

DLT; distributed ledger technology; ledger; blockchain; framework; regulation; policy

Disclaimer

Information for this report have been gathered from a substantial number of sources, including in-person interviews and desktop research for a large number of jurisdictions. While every reasonable effort has been made to verify the source and accuracy of the data collected, the research team cannot exclude potential errors and omissions. This report should not be considered to provide legal or investment advice. Opinions expressed in this report reflect those of the authors and not necessarily those of their respective institutions. Some contents of this deliverable may involve patents.

The Focus Group does not take the responsibility of identifying patents.

Working Group Leader:	Alexander Chuburkov Association for Development of Financial Technologies Russian Federation	E-mail: chuburkovalex@gmail.com, alexander.chuburkov@fintechru.org

Co-authors: **Alexander Chuburkov:** Alexander is an expert on standardization and regulation at the Association for Development of Financial Technologies (Russia) and a chief legal Officer at QIWI Blockchain Technologies LLC (Russia). He is also a national expert on international standardization GOST-R, Russian Technical Committee 26 for standardization "Cryptography and security mechanisms" (TC26), ISO TC307. His research interests include corporate governance and finance, financial regulation, and protocol design. E-mail: chuburkovalex@gmail.com

Artem I. Levashov: Artem is a specialist of the Digital Law Department of the Distributed Ledger Technology Center at the “Saint-Petersburg State University”. At the same time, he is practicing as an IP/IT/Media lawyer in “Northwest Consulting and Data Protection Office” LLC (Saint-Petersburg, Russia). E-mail: artem.i.levashov@gmail.com

Dr. Andrew Khramtsovsky: Dr Andrew Khramtsovsky works as a records and information management expert at Electronic Office Systems LLC (Moscow, Russia). Before switching to records management, Dr Khramtsovsky was engaged in aviation science for many years, IT and programming. He is a national expert in ISO and a translator of ISO standards. E-mail: AKhramtsovsky@gmail.com

Dr. Natasha Khramtsovsky: Dr Natasha Khramtsovsky is an experienced archivist, records manager, consultant, educator and translator of ISO standards. She works as a senior records and information management expert at Electronic Office Systems LLC (Moscow, Russia). She is a national expert in ISO and ITU, a member of ICA and ARMA International. E-mail: sspchram@tochka.ru

Grigory B. Marshalko: Grigory is an expert of the Technical Committee for standardization "Cryptography and Security Mechanisms" (TC 26), Moscow, www.tc26.ru. Grigory is the author of a number of scientific papers in the field of information security. See http://m.mathnet.ru/php/person.phtml

Ismael Arribas: Ismael is worldwide entrepreneur. Legal education and founder of Kunfud, International Security Mercantile Agency specialized on Independent Compliance. He is an accredited expert at Standards Developing Bodies for Blockchain and DLTs, a founding member of INATBA, mentor and founder of various startups like Lumiversity and Kronosa Alliance. E-mail: ismael@kunfud.com

Javier Ibáñez: Javier is a Professor of Commercial Law, Chairman of the Legal FinTech Observatory and Head of the Garrigues Company Law Chair (Comillas University, Madrid). He is the co-founder, board member and research head of Alastria (Spain's public permissioned Blockchain).

Jay Wack: Jay is the president of Tecsec, Inc. and crypto & cryptographic key management and digital currency expert. Jay serves on the ANSI X9 board and is an active member of ISO, IEEE, and CIGRE security working groups. Jay co-authored AGA 12's SCADA report and was awarded multiple patents in security and cryptography. E-mail: jayw@tecsec.com

Jörn Erbguth: Jörn is a consultant on blockchain and GDPR with a legal and computer science background who is a PhD candidate at the University of Geneva and also teaching at the Geneva School of Diplomacy. E-mail: joern@erbguth.net

Leonardo Paz Neves: Leonardo has a PhD in development from the Rio de Janeiro Federal University. He is an International Intelligence Analyst at the International Intelligence Unit from the Getulio Vargas Foundation (FGV) and Professor at the International Relations Department from the Ibmec College.

Patrice A. Lyons: Patrice is general counsel at the Corporation for National Research Initiatives. E-mail: palyons@bellatlantic.net

Patrice Payen: Patrice has more than 20 years as security engineer and risk, compliance & privacy specialist at Symantec. E-mail: Patrice_payen@symantec.com

Phillip H. Griffin: Phil is the owner of Griffin Information Security, a consulting practice in Raleigh, North Carolina, USA. E-mail: phil@phillipgriffin.com

Richard O'Brien: Rick works to increase the velocity of funding and collateral by developing technology and operating rules that militate the risk of synthetic identity fraud. He is the founder and CTO of Payment Pathways, Inc. E-mail: rick@paymentpathways.com

Tux Hu: Tux Hu is chief scientist at Starwin Capital which is located in Shanghai, China. E-mail: zhen.hu@starwincapital.com

Contributors: **Dmitry S. Maslyakov:** Dmitry is an expert on fintech and interbank payment systems. He has a broad experience as an analyst, solution architect and consultant in projects for financial institutions. E-mail: dsmaslyakov@mail.ru

Emilio Dávila González: Emilio is the Head of ICT standardisation sector within the European Commission. He works in the unit dealing with blockchain and innovation within Directorate General for Communication Networks, Content and Technology (DG CONNECT). He is responsible of coordinating ICT standardisation strategies, liaising with Standards Development Organisations active in ICT and, in particular, building bridges between research and standardisation and how standardisation contributes to innovation. In this capacity, Emilio is following up and participates in international standardisation technical committees related to blockchain. Emilio has also followed for many years international standardisation activities related to intelligent transport systems and connected and automated vehicles.

Kirill Bernevega: Kirill has an LL.M from the Higher School of Economics (Russia). He is an independent expert and practicing IT & IP lawyer. He was engaged in advising and managing legal projects for different tech companies. Before that had experience as an expert in competition authority. E-mail: berneveg@mail.ru

Prof. Volker Skwarek: Volker is Professor at Hamburg University for Applied Sciences. He has many years of experience in academic research on DLT systems for improved data security in distributed systems. Parts of his and his team's expertise also covers smart contracts and their legal aspects in business applications. In this role, he is also convenor in ISO TC 307 for WG3, smart contracts.

Stanislav Vazhenin: Stanislav as a PwC senior associate is responsible for tech deals and strategy projects at PwC Russia and Eastern Europe. His knowledge and expertise in venture capital and Private equity helped PwC to close some of the largest deals in the region in 2019. E-mail: stasvazhenin@gmail.com

Stiepan Aurélien Kovac: Stiepan is an ISO SC27 WG2 expert, administrator of QRCrypto SA, 1700 Fribourg, Switzerland, a company actively promoting quantum-resistant cryptography. E-mail: stie@itk.swiss

CONTENTS

Page

Technical Report FG DLT D4.1

Distributed ledger technology regulatory framework

1 Scope

This technical report discusses key features of distributed ledger technology (for the purposes of the report, the word "Blockchain" construes distributed ledger technology, or DLT) and its associated regulatory challenges. Examples of approaches that users, regulators and solution providers could use to address the regulatory challenges facing DLT are also discussed.

2 Terms and definitions

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

3 Abbreviations

AI	Artificial Intelligence
AML	Anti-Money Laundering
CA	Certificate Authority
CADES	CMS Advanced Electronic Signatures
CNIL	Commission Nationale de l'Informatique et des Libertés
CRL	Certificate Revocation List
DAO	Decentralized Autonomous Organizations
DPIA	Data Protection Impact Analysis
ECC	Excise Control Code
EdDSA	Edwards-curve Digital Signature Algorithm
eIDAS	electronic IDentification, Authentication and trust Services
EIF	European Interoperability Framework
GDPR	General Data Protection Regulation
ICO	Initial Coin Offering
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Intellectual Property
IPO	Initial Public Offering
KYC	Know Your Customer
P2P	Peer-To-Peer
PII	Personally identifiable information
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PoA	Proof of Authority

SC	Smart Contract
SDG	Sustainable Development Goal
SEC	Securities Exchange Commission
SSI	Self-Sovereign Identity
STO	Security Token Offering
TCP/IP	Transmission Control Protocol/Internet Protocol
TGE	Token Generation Event
TLS	Transport Layer Security
TTP	Trusted Third Party
ZKP	Zero-Knowledge Proof

4 Introduction

This report considers key properties of DLT that are common amongst the diverse approaches to DLT. It aims to bring into focus the topics concerning DLT regulation. By supplying practical recommendations to users, regulators and technologists, this document seeks to aid in the mitigation of potential risks associated with DLT.

Clause 5 outlines DLT features and regulatory challenges. Each sub-clause corresponds to an essential feature of DLT, describes specific problems and risks as well as recommendations on how stakeholders might address them

This document contains the DLT Regulatory Framework, the key properties of DLT and regulatory challenges (see Table 1) and recommendations for users and regulators.

We mean to indicate governance (strategic guidance) and regulatory (legal and compliance) issues that could arise in early adopted use-case implementations of DLT. The technical properties of digital entities/objects are crucial for enforcement of the rule of law (governance, liability, intent, attestation of accuracy and chain-of-custody).

5 DLT regulatory issues

In scope, are the following concerns from the analysis of the properties of DLT:

Table 1 – DLT features and regulatory challenges

Feature	Examples of regulatory challenges
Distribution, shared ledger (no central repository) [b-Yaga]	1) Applicable law with respect to nodes established in different states; 2) Legal subjects in multiple jurisdictions; 3) Distributed storage solutions to meet the requirements of production environments; 4) Interoperability requirements; 5) New civil or commercial-law forms, organizations and contracting; 6) Protection of secrecy in open environments.
Autonomy and responsibility	1) Legal smart contract definition and enforceability (valid source code execution); 2) Boundaries of anonymity; 3) Applicable law; 4) Liability of smart contract managers (SC layer governance); 5) Intellectual property of code.
Tamper evidence and resistance	Regulation that requires the correction or removal of data in the ledger, for example: 1) data protection laws / right to be forgotten; 2) content that infringes on third parties' rights (e.g. copyright, trademark etc.); 3) illegal content.
Incentive mechanism and digital assets [b-FINRA, b-Yaga]	1) Coin, token, tokenization legal common (UNCITRAL) definition; 2) ICO definition and minimal requirements for investor protection; 3) Crypto asset/token financial system: legal concept and boundaries; 4) Supervisory policies and procedures in accordance with applicable rules [b-FINRA].
Openness and transparency/ anonymity	1) AML issues, secrecy leaks, personal security [b-FINRA]; 2) Anonymization (no name/encrypted users vs KYC) and pseudonymization [b-EU-a].

There are five categories of laws addressing DLT systems:

- Laws that address the DLT systems themselves, like intellectual property (IP) (patent, copyright) of software code, communications laws and laws that regulate the mining for a DLT system.
- Laws that address the governance of DLT systems. This includes, for example, the recognition of DLT governance, conflict of laws, liability and enforcement of decisions on a DLT system.
- Laws that affects some or many use-cases of DLT. This includes crypto regulation and token-economy laws, anti-money-laundering and privacy laws, consumer law protection regimes, and anti-fraud laws as well as laws allowing law enforcement to carry out certain measures or use certain tools in a digital environment.
- Laws affecting civil liability and the law form of consortia governing the DLT, which is essential for the optimal governance of permissioned systems
- Laws affecting the issues concerning different layers within the DLT structures, such as EU eIDAS Regulation and similar currently enforceable laws on electronic signatures worldwide; laws on software IP; laws on DLT-components technical specifications.

The correspondent challenges refer to matters such as:

1. Civil and criminal liability in the blockchain network control, and other sources of responsibility from a public-law perspective (eg. administrative compliance taxation and even constitutional-law related issues)
2. The control management supervision of the network participants s (human or not), including developers administrators, consortia/community managers and legal persons involved within.
3. Authoritative sources of records and data;
4. DLT-record legal proof;
5. Personal data protection compatible with existing regulations.

5.1 Property 1: Distribution and ledger sharing

Distribution is a network configuration where every participant can communicate with one another without going through a centralized point. Since there are multiple pathways for communication, the loss of any participant will not prevent communication. This is also known as *peer-to-peer (P2P)* **distribution** which implies operation without a central data repository. The characteristic of the term "distributed" in a DLT context is based on data sharing among multiple systems that are set in different locations. **Distribution** entails P2P interaction and its corresponding contractual or extra contractual liability

The anatomy of a DLT system could be described as a system of layers consisting of protocol, orchestration, business, data and network layers. Two global standards define orchestration among various elements in various layers.

A distributed process occurs across multiple nodes interacting in a P2P mode. In this context, decentralization means that there is no central responsible unit coordinating the inter-node action or contracting; thus, there is no central supervision or authority, though there may be several responsible units within a permissioned DLT context.

Decentralization can mean that different types of nodes with different powers and attributions may decide differently. All nodes share the same data and execute the same smart contracts but the instantiation and execution of P2P transactions comes from eventually responsible nodes or represented persons in enforceable contracts, thus generating contractual responsibility.

Ledger sharing implies a methodology for data storage and retrieval in a manner that protects the sequence and fidelity of the stored data from any alteration whatsoever prior to its retrieval. Data protection and constitutionally protected related rights (honor, association, privacy, asset property and intellectual property (IP)) are directly concerned.

Distributed ledger technology (to which blockchains belong) does not only combine "distribution" and "sharing" but also requires using public key asymmetric cryptography, distributed databases (large-scale data storage and processing), peer-to-peer communication (P2P network), consensus mechanisms and other technical innovations, which pose regulatory challenges, mainly company and contract law related, without prejudice to sectorial laws concerned (banking, insurance, capital markets, amongst others). Competition law and consumer law are also directly concerned by distribution and sharing, as vendors and other competitors work collaboratively to produce the infrastructure and devices within related layers, though they compete in the distributed application layer when introducing use cases for their industries.

Distributed ledger technology is designed to support tamper-resilient and close to immutable, decentralized, shared ledgers and is based on strong cryptography. Blockchain technology does this by combining data blocks in a chronological order into a specific data structure in the form of a cryptographically linked list. Blockchain technology is a tamper-resilient and immutable, decentralized, shared ledger using cryptographic functions that combine data blocks in a chronological order into a specific data structure in the form of a linked list. Shared ledgers do not solve the issue of data accuracy but can only prove who has written the data at what time.

When distributed consensus algorithms are used to add data that can subsequently trigger the execution of code retrieved from blockchains, such as smart contracts, the automatic execution of business logic is ensured. A blockchain or "shared ledger" is a decentralized (multi-centered) infrastructure that is a new distributed computing paradigm which has a mechanism of enforcement adhering to operating rules in a manner persistent and consistent in a variety of settings.

5.1.1 Introduction of the property

"Distributed fashion" permits associative models of auto-governing rules to facilitate the operation of a useful, trustless and efficient system. Trustless means that the technology does not require relying on trust of a single entity or participant. This “distributed fashion” property encompasses all matters of concern that might exist between liable entities and an allowance for the opportunity to change their governance protocol, under specific rules, which legitimizes this change of a protocol layer.

The scope of this property includes defining regulatory boundaries and gateway protocols to achieve liability isolation among participants. Such isolation is distinguished by the context of multi-lateral or bilateral data exchanges. Thanks to these properties (distributed fashion and shared ledger), interoperability with another DLT ecosystem can be proposed by either a participant network, a data owner or by both of the aforementioned – to change the protocol layer and adjust it in accordance with the prevailing rules.

The mapping in Table 2 shows a diverse array of governance models to DLT implementations which are a derivative update to that work.

Table 2 – Protocol governance models/Governance decision-making process models (partial list)

Locus of control / Trust model	Decision-making process	Meaning	Examples of projects' platforms
Ranging from distributed among multiple governances to Negentropic	Cooperative	Protocol change proposals are provided and approved on a cooperative and voluntary basis due to absence of a central authority. Contentious proposals run the risk of fracturing the network resulting in a permanent split.	Bitcoin
Centralized, autocratic	Autocratic, arbitrary	Decisions over changes on protocol rules are taken by a single entity (e.g., a person, company, mining pool, etc.).	Ripple, Project X, Hyperledger
Centralized: With two or more governance tiers	Hierarchical	Individuals have the ability to propose changes but recognized leadership (e.g., foundation or a committee in control of a key code repository) all but ensures protocol changes will rely on the consent of the leaders.	Ethereum Foundation
Centralized: With conditional governance tiers	Plutocratic unequal horizontality	Protocol change proposals are voted on where each vote is weighted by the importance of each proposer or voter. In the plutocratic case, substantial weight is given to a minority of voters (e.g. due to high ownership share of the weighting asset).	Alastria
Decentralized democratic autonomous agency	Horizontal	Protocol change proposals are voted on with each vote weighted by the importance of each proposer or voter. In the democratic case, a minority of voters do not have substantial weight in vote outcomes.	Democracy.earth
Futarchy	Indirect consensus	Decision-making operates through a metric pre-defined by its stakeholders. Prediction market models are used to determine which policies will have the most positive effect.	Aragon, Tezos, Gnosis

Locus of control / Trust model	Decision-making process	Meaning	Examples of projects' platforms
Federated	Coalition/ collective partnerships	A group of agents vote on protocol alterations linked by a horizontal relationship scheme. Members of a federation need not have equal voice/power nor even necessarily known to each other.	Verified.me

Distribution implies that **solutions** have an initial system design and a governance model to alter it. There is a conflict between:

- Having unfettered (unrestricted) freedom to deploy and use a DLT-based framework under a peaceful association as a constitutionally acknowledged human right; versus;
- Having limitations/boundaries of right(s), where some guidance (rules and policies) places restraints on DLT-based framework deployments and usage activities (e.g., priori functionality descriptions are associated with conditions for use by users, providers, participants, owners, etc.). When imposed by governance convention, the purpose of restraining actions is to ameliorate outcomes that may be harmful to groups or interests.

[b-Rauchs] distinguishes three levels for altering the protocol governance layer which is, in functionality, a hierarchical critical configuration based on: proposal, funding approval and implementation. The different proposals entail governance alternatives of participation and authorization to restrict the exercise of individual participation (voting, property selling, voluntary contribution, debate on governance, etc.), as specified in network foundation documents.

The key regulatory challenges associated with this property are:

- Applicability of existing law with respect to nodes established in different states;
- Legal responsible subjects in multiple jurisdictions, competition and failure-handling issues are relevant within a DLT governance context. To this extent it is worth mentioning that there is a relevant distinction between the incident management model and the incident governance model;[1]
- Distributed storage solutions to accomplish legal requirements of production environments;
- Legal accomplishment of interoperability requirements. The heterogeneity of DLT devices, operating systems, programming languages, node managers and networks pose a huge challenge within different legal areas;
- New digital civil or commercial-law forms such as multilateral consortia agreements, organizations such as DAOs and decentralized e-contracting including financial system contracts for banking, stock markets and insurance purposes;
- Protection of secrecy in open environments in accordance with existing data protection regimes in force in different jurisdictions. Security related issues should be addressed as well as far as they concern integrity, confidentiality, enforceability, availability and usage of networks with variable scope in different jurisdictions. Some constraints may work at cross-purposes and require multiple protections to satisfy criteria drawn from different governance authorities;
- Cross-border transfer and data localization: collecting data, retaining data, analyzing data, deleting data and sharing data. Data storage and privacy and personal data may fall under regulatory purview if derived from other non-protected data attributes: directives, regulations and jurisdictional impact on personal data protection;

[1] Generic standards for information sharing exist, such as ISO ISO/IEC 27010, 20614, 20247 and 19592. However, no incident management model or information standards yet exist for blockchain and DLT incident management, nor are there any standards on how blockchain and DLT could be used to support the incident management model.

- Perhaps, the main legal challenge associated with DLT addresses the identification of responsibility in distributed systems. Present legal systems often assume hierarchical control of systems in order to attribute responsibility accordingly;
- Multi-jurisdiction and arbitration: Conflicts to be resolved automatically, or autonomously, while maintaining the persistence of the framework and deciding which conflicts are destined for off-chain resolution or off-ledger resolution. Different territorially applicable laws can enter into conflict with these solutions. Court orders from one jurisdiction may supersede internal blockchain governance as well as other court orders. Possible solutions like setting up arbitration agreements or defining the applicable law in some kind of contract between the participants may not be recognized by all jurisdictions;
- Market Competition: Antitrust and anti-competition law.

5.1.2 Approaches and/or recommendations

We recommend to efficiently combine the aforementioned approaches within the scope of future international working group legal prospection with regard to significant findings by specialized doctrine and jurisprudence and in accordance with governmental national or regional forthcoming sectorial approaches, in particular within these fields:

- Civil and criminal liability for blockchain distributed control;
- Decentralized controllers/managers (human or not);
- Authoritative sources of records and data;
- DLT-record and other related digital sources of legal proof.

5.2 Property 2: Autonomy and responsibility

Autonomy and responsibility imply having the right or power to choose how to act and may result in legal liability. Invoking this choice may be an essential consequence of having the capability to exist independently – an essential consequence of attributing, ascribing or assigning independent existence to machines [b-Ibáñez-a].

5.2.1 Introduction of the property

Transactions on DLTs can be executed autonomously. This means that these transactions only depend on the conditions set in the DLT. The code is protected against interferences. Smart contracts (SCs) can automate some of the processes typically associated with a legally binding contract [b-Raskin].

SCs can be used to implement on-chain governance to human decisions in networks, organizations or entities within DLT systems. Any voting process can set the rules by SCs that can be traced uniquely.

The design of SCs allows for the definition and adoption of rules in order to perform transactions recorded in DLT. Decentralized autonomous organizations (DAOs) which are developed and upgraded by users can model autonomy for decentralized communities. The proliferation of DAOs and autonomous models of governing people, entities, things and processes demonstrates effective orchestration of other components.

With the rise of awareness for data privacy, SCs often only process validation metadata to prove the correctness or the valid exercise of rights to access privately stored data (e.g., in Self-Sovereign Identity (SSI) [b-Bundes Block]).

5.2.2 Challenges associated with this property

Contract automation has possible legal effects. SC autonomous execution is limited to assets stored on-chain. All other enforcement of code agreements inside the SCs ("law" [b-Lessig-b]) needs to take the traditional approach of enforcement.

An SC can also be a representation of a legally binding agreement executed on a blockchain wherein the code entails contract execution.

A smart contract with legally binding intention (also referred to as "legal SC") is a possible representation of a legally binding SC agreement executed on a blockchain.

The legal interpretation of the contract could differ from that brought by code execution; then, code can be legally binding, except when it isn't [b-Peterson], in accordance with applicable law.

Code execution must not infringe mandatory laws. If that were the case, remedies should be pre-set on-chain (SC self-correction, integrated automated arbitration or dispute-resolution mechanisms) or off-chain (external compensation). The code of SCs often needs maintenance (e.g., special permissions to replace part or all the code with a new version). Governance must prevent the abuse of this power.

Dispute-resolution and compensation widgets can be implemented to avoid conflict with laws:

a) On-chain, as part of SCs;
b) Off-chain (private arbitration, which is still preferred by courts by virtue of being flexible).

Trust in DLT oracles: SCs can only securely access to information on-chain. Thus, external information should only be incorporated through trusted third parties or sources of data called DLT oracles.

Interoperability: Information from other DLT systems can be integrated through DLT oracles or through securely interconnected different blockchains.

5.2.3 Regulatory challenges

5.2.3.1 Legal smart contract definition and enforceability, and valid source code execution

Subsidiary off-chain enforcement of SC terms and conditions may be required in cases of breach of SCs with contract-law structure (“legal SCs”) requiring restitution [b-Ibáñez-a].

Boundaries of anonymity, to solve the conflict between privacy rights and public-law order. Anonymous and pseudonymous transactions: Smart contracts enable to conceal or hide the identity of the transacting entities. Even though this aspect is desirable from a privacy viewpoint, it might facilitate crime, or impede the application of transparency laws (namely AML). Ensuring privacy only to low-cost transactions might be a solution there. Another approach is controlled pseudonymization of data owners, thus keeping data traceable in a limited way.

Enforceability of legal SCs (SC with contract-law structure) [b-Ibáñez-a]. While the SC code can self-enforce transactions on DLT-managed assets, other contract terms require traditional enforcement, in particular when its breach requires restitution. When SCs are used pseudonymously or in an international context, conventional enforcement might be difficult.

Applicable law: SCs should fix applicable laws and legal forum / arbitration though consumer or investor tutelary rules. International private law might still compel to apply local laws or forum. Current pseudonymity could be private enough to hinder conventional enforcement and at the same time not be private enough and therefore break privacy laws.

Software developers of SCs, as parties in blockchain nodes, may incur Legal liability (criminal and civil) – this especially applies in Proof-of-Authority (PoA) governed networks [b-Ibáñez-b].

Intellectual property (IP) rights on SC code. Such code is often open-source, but it is possible to include a fee for using it. Thus, IP rights and anti-competition laws apply [b-Alastria]. Special provisions can be set by combining SCs with IoT [b-ISO/IEC 30141] or AI.

5.2.3.2 Automatic decision-making

SCs differ from automated decision-making (ADM) in AI. Whereas ADM in Deep Learning can be very complex, provide little transparency and includes random input in the training phase, SCs are simpler and provide high levels of transparency, at least to people skilled to read the code. Still, principles currently being discussed for ADM in AI may need to be applied to SCs [b-Larus]. Article 22 of the GDPR might also be applicable [b-Finck]. The GDPR requires at least the possibility of human intervention of the “controller” (see section 5.3.2.1.3 for clarifications of this concept).

In case of SCs operating on a permissioned blockchain, validators or permissioned nodes with full autonomy will have duties of full performance of SCs.

5.2.3.3 Limitations of legal liability for actors who play the key role in information system operation

The legal problem here is a formulation of corpus delicti with regard to technological features of DLT based on information intermediary theory.

One of the main mechanisms for ensuring compliance with applicable laws in a digital environment is a regulation of information intermediaries and information service providers. In general terms, these rules indicate limitations of liability of information service providers in situations where they do not affect content of the network as well as take actions to prevent third parties from accessing information on legitimate requests from rights holders and state authorities. At the same time, the law enforcement practice in some states also consider other criteria for bringing information intermediaries to take responsibility such as receiving profits from information posted or a failure to take preventive measures to combat offenses [b-Saveliev-a]. Moreover, researchers have noted a tendency towards expanding the limits of responsibility of intermediaries and moving towards mandatory monitoring of the network [b-EDRi]. Such legislative changes are important not only for a direct consequence of their application but also for the political and legal component of their content; one of the most effective and popular ways to regulate information networks at the moment is shifting responsibility from end users of networks to administrators.

Thus, the main direction of regulation of information networks is based on establishing an administrator who creates an information ecosystem around them, setting the rules for its use, as well as features of identification and verification of its participants. In contrast, a key feature of peer-to-peer networks is interaction of users directly without contacting a certifying third party (the administrator-provider of information services) [b-Raval]. As a result, relationships of users without intermediaries are becoming similar to traditional private law relationships. In theory, each member of the DLT network has equal legal rights and is guided by his own interests and is independently responsible for his actions.

However, unlike the real world civil legal relations, the standard of good faith and due diligence for DLT system users is much higher because features of the architecture of distributed networks predetermine some characteristics of transactions committed in it - for example, its abstractness, as well as the locality of the legal effect (only within the relevant DLT). These features require coordination with national legal systems, both in terms of understanding the nature of regulatory transactions, and the legal significance of making entries in public ledgers [b-Russian Fed.-b]. If there are no such features, control of relations arising in a DLT network with instruments of contractual law, even if detailed, remain under threat of requalification of legal relations in the event of a dispute and applying different rules to them than the parties have foreseen, based on imperative nature of certain rules of the applicable law and order public policy expressions of the legal system (for disputes with a foreign element).

Additionally, this regulation raises the question of how and by whom the rules of user interaction between the DLT network nodes will be developed and established. In the practice of managing DLT projects, the regulation of related legal relations, we observe cases of deviations from the principles of decentralization. So, at least when it comes to making key decisions about existence of the system, for example, about its launch, scaling or radical change (implementing the so-called “hard fork”), a certain degree of centralization and formation of the will of the participants is required. It seems that special analysis of such centralizations makes it possible to detect “exit nodes” [b-Sidorenko], by regulating activities of which, it is possible to ensure legal regulation of information system as a whole. Moreover, with the development of a DLT network and its increasing interaction with the surrounding reality, more and more nodes of this kind arise and consequences of their decisions are becoming increasingly critical for the system as a whole.

Considering the above, it is necessary to determine a circle of persons ensuring the operability of DLT networks and that have a significant power to impact the procedure for their use. It seems that in most such systems the following play a key role:

- Agents that establish technological and organizational rules for a specific network (developers, administrators);
- Agents most actively involved in formation and validation of blocks (miners, minters and validators);
- Agents who, due to nature of a specific electronic platform, ensure its use (facilitators).

At the same time, the identification and description of a system nodes circle, which technologically ensures its functioning, directly depends on type of a deployed DLT. Due to the fact that in private DLT there appears a figure of the network owner who controls the formation of a register of blocks of transactions, it is logical to assume that the regulation of its activities will ensure compliance with applicable laws. A similar approach can be extended to validators of consortium DLT where they not only generate blocks but also check the validity of transactions included in blocks. It is necessary, however, to consider that initial rules of the DLT are normatively formulated and technologically implemented by developers and administrators of the relevant platform and therefore their participation in the network can also be used for state control.

Regulation of the activities of the above-mentioned persons is considered to be the most effective way to ensure the legitimate functioning of DLT networks. First of all, such regulation should be carried out by influencing the network administrator, who after the launch of the system retains ability to influence its content and development in one way or another. Special requirements may be imposed to persons administering DLT systems, such as localization within the country where a person performs such activities, similar to some information service providers [b-Russian Fed.-a]. A more stringent regulatory option is licensing of activities and creation of a system to control its implementation, as is practiced in a number of countries in relation to administrators who intend to conduct an ICO (initial payment offering). If the DLT system is designed in such a way that administrative functions are actually autonomous, the development of mandatory technical activity standards seems to be a promising way.

Failure to comply with such standards may reasonably lead to the revocation of a previously issued license for bringing the administrator to responsibility (as an independent basis or element of the corpus delicti in case of illegal actions of users) or for shifting the burden of proof to the administrator in case of a dispute regarding the civil rights of the user or a third party.

Also, it should be noted that any system built on DLT includes not only, directly, a distributed ledger but also a "software shell" which is a software application that allows users to interact with each other and with the ledger. If a fundamental change in rules of forming a chain of blocks is a rather difficult task that requires a large level of interaction from ordinary users, then the application level software can be updated in ways that are slightly different from those used in classical information systems.

Consequently, in addition to ledger decentralization, centralization occurs in providing users with an interface for interacting with this ledger. In this regard, we can make at least two conclusions. Firstly, in terms of providing the ability to use application software between administrators of the DLT network and its users, there are typical relationships for information networks that can be qualified as licensing services or as providing remote access services [b-Saveliev-b].

Secondly, it appears that it is on the application software level that users can be identified and verified, which, given the basic distribution of responsibility arising from the peering nature of the network, will solve many problems of regulating relationships in the current information environment.

5.2.4 Approaches and/or recommendations

Optimal third-party protection requires policies setting on-chain dispute resolution tools on a case-by-case basis prior to an off-chain solution. Associative initiatives within the scope of International Consumer Protection and similar regimes are recommended to complement the aforementioned policies.

Companies using SCs have to comply with the existing regulation. Consumers might be able to benefit from an increased level of trust that does not depend on the trust in the company.

In order to increase the trust when SCs are used, e.g., for managing tokens, a certification of smart contracts can be demanded by law.[2]

5.2.4.1 DLT & corruption

Anonymity and pseudonymity in permissionless blockchains can facilitate criminal purposes like tax evasion, bribery, money laundering or terrorism financing. However, chain analytics can be used to follow transaction on pseudonymous blockchains like Bitcoin. Prosecution of crimes is easier where

[2] Malta currently requires the certification of smart contracts used for ICOs (ITAS).

transactions require automated permission or participation requires identification. The same can be said about transparency.

Blockchain can also be a tool to increase transparency for public institutions. However, transparency is limited to the information stored on chain or validated by means of entries on the chain like hash-values.

Natural persons can be identified with transparent transactions, however, increased transparency can have a negative effect on privacy. When the transactions concern business transactions, increased transparency can impact business secrets.

Blockchain/DLT is promising in the context of inherently distributed business and governance activities where traditional means are not working.

- Anti-corruption and pro-transparency measures should be considered early at the design stage taking into account the intended application of the solution. At present, however, the focus of governmental actors is mostly on privacy (including transaction privacy) protection, which is quite beneficial for corruption-supporting applications of blockchain.
- The lack of a designated owner or responsible person in permissionless blockchains combined with trans-jurisdictional operations hinders public oversight and law enforcement.
- Properly designed SCs may ensure fair access to goods or services with no interaction with potential criminals. But, they could also be used for collecting bribes. Then, authorized SC removal and vetting systems are needed in public permissioned chains.

5.3 Property 3: Tamper evidence and resistance

5.3.1 Introduction of the property

DLT provides a conceptual model for providing tamper resistance that is based on:

- Cryptographically signing the entries by the appropriate private keys;
- Chaining the data with cryptographic hashes so that a single data entry cannot be modified without modifying many subsequent entries;
- Sharing the data with multiple users where a consensus algorithm takes care of synchronizing the stored information.

There is no measure for ensuring that a single node contains a complete set of transactions. Complete tamper resistance can only be reached by having so many decentralized nodes that no one would be able to convince all of the nodes to tamper with their ledgers.

5.3.1.1 Technological basis: Asymmetric & symmetric cryptography

Digital signatures are created using the private key component of a public-private key pair. A digital certificate contains the public key component of an identified subject that is signed by a certificate Authority (CA) to issue a certificate. The CA-signed certificate binds a subject identity to a public-private key pair.

Trust in the identity of the subject whose signature can be verified using the certificate public key depends on the confidentiality of the associated private key. The certificate subject must maintain sole possession of the private key. If poor key management is practiced by the subject, it is possible for an attacker gaining possession of the private key to impersonate the subject and to forge their signature.

In a permissionless ledger, there may be no requirement for using PKI-associated certificates. It is possible to use only the public key to verify the validity of a signature created with the associated private key. When public-private key pairs are not associated with a PKI, signatures created with a private key can be verified using the associated public key to gain data integrity assurance but no origin authenticity or non-repudiation services are provided. These services require a PKI.

In permissioned ledger environments, PKI-based signatures may be required so that participants are able to comply with legal or regulatory requirements. These requirements may include "Know Your Customer" (KYC) and Anti-Money Laundering (AML) rules that are commonly applied to financial services organizations. In this context, PKI may be used both for digital signatures and for access control to a ledger platform with an authentication protocol such as Transport Layer Security (TLS).

5.3.1.1.1 Signature Processing

Signature verification is used to determine if a signature on some data content is valid. Verification is performed by signing the content again and comparing that result to a presented signature. If the two signatures match, the signature is considered to be valid. Content is often hashed before it is signed and the signature is then applied to the hash. In this case, signature verification also requires recalculation of the hash of the content.

In clause 12.5.1 of Recommendation ITU-T X.509, the basic public key certificate checks include verifying that the signature of the CA is valid. Other checks follow, including ensuring that dates in the certificate are valid, that the certificate has not been revoked and that the private key component is being used for a purpose authorized by the issuing CA such as for signing certificates, signing data or for data encryption. In the case of DLT, a relying party accepts all liability for trusting a certificate-based signature as is typical for other cases of PKI.

Some organizations that participate in a DLT system may require compliance to a security policy requiring that whenever a certificate is used, its signature must be verified and checked to see that it is fit for purpose (e.g., contains valid dates, uses approved algorithms, includes required extensions, that it not be revoked, etc.). The security policy may also require that the certificate path be validated back to an organization-trusted root. Certificate path validation must be used to provide assurance to the relying party that the identity of the signer can be trusted.

DLT systems may require that private extensions be included in certificates used to access their platforms and they may impose additional verification requirements. Vendors may offer a choice of signature algorithms and key lengths that can be used on their platforms. The available choice alternatives may conflict with those that comply with an organization’s security policies. Vendors may impose certificate validity periods that conflict with the key management requirements of an organization for periodic key rotation. In order to participate in a given DLT, an organization may need to obtain and manage exceptions to its security policies. The validity period in an X.509 certificate allows a relying party to make decisions about trust in a signature. These 'not-before' and 'not-after' dates apply to the public key signed by the certificate issuer and to the associated private signing key. Once a certificate expires, the private key should no longer be used for signing. At any time, signatures created outside of the validity period using the private key should not be trusted.

The public key can be used to verify and validate signatures that were created during the certificate validity period. Verification and validation can be performed at any time, even outside the validity period, so long as the date and time of the signing is known. A DLT timestamp, although not proving a precise time, can provide this information.

5.3.1.2 Challenges associated with this property

- Technological challenges, i.e., managing technological change;
- Regulation that requires the correction or removal of data in the ledger;
- Electronic and digital signatures are regulated in some countries (e.g., by eIDAS in the EU). It is being discussed to extend this regulation from PKI to DLT. Some courts already recognize DLT-based proofs [b-Zhao].

5.3.1.3 Technological challenges

Cryptographic keys used in DLT are subject to change. This may be due to an organization’s security policy or to its certificate or key management requirements. Approved signature algorithms may become deprecated and key length requirements may increase over time. As new algorithms become available they may replace existing ones to achieve better performance or greater protection.

This has been the case for other systems and protocols such as TLS, which recently deprecated use of a widely used RSA key management technique and approved the use of EdDSA, a more recently developed family of digital signature algorithms. EdDSA is also used in crypto currency, blockchain and ledger systems. All cryptographic algorithms are subject to obsolescence. This has been the case for hash algorithms such as MD5 and SHA-1, which were once used for signatures in PKI but have since been replaced by algorithms such as SHA-2. As certificates expire they must be renewed or replaced based on an organizations policies. As a rule, CA certificates must be updated well before they expire so that this process can be performed without disruption. These updates may cause transactions that span multiple blocks to rely on signatures that use different algorithms or key lengths. So, it is important that DLT applications are agile and that DLT platforms are designed to expect change. Moreover, from a general point of view, in blockchain, blocks are not required to be signed.

Also, the syntax’s CAdES is not the unique way moreover with eIDAS the preservation of electronic signature is adjusted to the limitations of the use of the DLT. Finally, regarding Recommendation ITU.T X509, although it is correct, it is problematic for validation of passed signatures or applicable to certificate revocation [b-Diaz]. ETSI EN 319 102.1 extends the algorithm to give a clear response to that problematic, and it is relevant that this standard is adopted in the European Union as well.

Furthermore, the coming development of quantum computing is expected to be disruptive. According to Michele Mosca of the University of Waterloo, quantum computers “will break currently deployed public-key cryptography, which underpins the security of DLT systems that rely on PKI, and could become a threat in the next 10 years knowing that commercial availability might be preceded by military availability”. More significantly, the PKI systems fielded today are about to become obsolete, in particular, those based on RSA and those with keys smaller than 4096 (or their ECC equivalents), and even those are approaching their end, all due to the quantum attacks offered by Shor’s algorithm [b-Bäumer]. This will force adoption and deployment of new signature algorithms that have been designed to be 'quantum-safe', or, resistant to quantum attacks. Consensus on which new algorithms should be safe to use as replacements is still being reached by researchers, governments and standards bodies. However, the time to start planning for changing signature algorithms is now.

The DLT system-reliance on PKI issue posed by quantum computers also applies to symmetric cryptography whenever it is used to store encrypted data on the blockchain and thereby, ensure its confidentiality and integrity. In effect, whereas large enough quantum computers will disrupt most existing standardized asymmetric crypto (with the notable exception of the ANSI standard for financial services X9.98 and the two stateful hash-based signature standards at the IETF), quantum computers will also affect symmetric cryptography in that, they will halve the key space due to Grover’s algorithm [b-Grover]. As a direct consequence of that, current 128-bit algorithms will be rendered useless and there will be no standardized equivalent providing 256-bit level security in the post-quantum scenario, for that would require 512-bit keys. Hence, this area is a work in progress (notably at ISO). The intermediary recommendation holds that when symmetric encryption is mandated by the system's design to store data on the blockchain, which is one of the paths to GDPR-compliance, 256-bit keys are to be used as a minimum for systems that are meant to last for more than 10 years.

5.3.2 Regulatory challenges

5.3.2.1 GDPR – Data protection

The European General Data Protection Regulation (GDPR) applies outside Europe in certain conditions e.g. when data subjects in Europe are addressed or monitored.

5.3.2.1.1 GDPR – Challenges

The GDPR requires a justification for processing of personal data and provides the data subjects with the right to be forgotten (Art. 17), the right to rectification (Art. 16) and the right to restrict processing (Art. 18). This can create conflicts with the immutability of DLT systems. The oblivion and erasure, however, is not limitless, existing only if the justification to store the data ceases.

The GDPR requires controllers and processors to have a processing agreement. Controllers are limited to select processors that are providing sufficient guarantees to comply with the GDPR (Art. 28). It is yet unclear how this has to be interpreted in the context of public blockchains and whether the code of a blockchain can serve as some kind of smart contract for the processing agreement.

The GDPR limits the transfer to third countries. Having nodes in third countries might transfer personal data to those third countries. However, publication is not considered a transfer to a third country, even when the data can be freely accessed from a third country [b-EU-c]. What does this mean for a blockchain with nodes in third countries? Does this privilege a public blockchain over a non-public blockchain?

5.3.2.1.2 GDPR – Personal Data

The GDPR does not apply to DLT when no personal data is processed. However, the definition of personal data goes far beyond what is considered PII. In other jurisdictions like the U.S., data that could be attributed to a natural person by the use of additional available information is already considered personal data.

A common way forward is to store the main data outside of a blockchain or on a sidechain and use the blockchain for verification, ordering and time-stamping. This is done by hashing the personal data. However, hashes of personal data may represent personal data themselves.

Typical pseudonymization scenarios, where only names or other identifiers are replaced by hashes (or even random numbers), are usually still considered personal data [b-Art. 29 WP]. When there is a certain context or some metadata stored with the hash on a blockchain, this can also be used to derive personal data. People who have knowledge of the hashed information will be able to connect the metadata with the data they have. Therefore, no metadata should be stored along with the hash that is not included in the information hashed [b-Erbguth-b].

Furthermore, hashes must have sufficient entropy, otherwise, the hashed data can be guessed. With Bitcoin mining, the calculation of hashes has become very fast. Added random data, also called salt, is often needed. When this random data is also used as a key to restrict access to the hash, then it is called pepper.

Zero-knowledge proofs (ZKPs) can be used to make sure that only non-personal data can be derived from an entry on a blockchain.

Encryption can be used to make it impossible to derive any personal data from a blockchain after the key has been deleted. However, storing encrypted personal data on a blockchain is like securing access to data by a non-changeable password which should be avoided [b-Grassi].

Although data protection authorities agree that these techniques substantially reduce the risks for data subjects, the French CNIL still regards them as being personal data with the exception of certain zero-knowledge proofs [b-CNIL]. The Austrian Datenschutzbehörde [b-Austria], however, while considering a case not related to blockchain, held that an effective protection against identifying a person can render the data anonymous, and that this is equivalent to deletion.

In addition to this legal uncertainty, anonymous data might become personal data in case of technological developments or when newly available external data becomes available which enables the identification of individuals with information stored on a DLT.

5.3.2.1.3 GDPR – Control

The GDPR puts obligations on parties in control of data processing. The French CNIL holds that users signing a transaction with their private key for a public blockchain are in control. When users are effectively in control and companies solely provide tools for writing on a public blockchain, the companies might not be responsible for data processing [b-Erbguth-a].

5.3.2.1.4 GDPR – Justifications

When there is a permanent justification to write personal data on a DLT, it can be stored there permanently. Consent can always be withdrawn and is generally not suitable to serve as a permanent justification. Possible permanent justifications can be the performance of a contract with the data-subject, legal obligation or compelling legitimate interest. In most cases, however, it will not be possible to obtain a permanent justification.

5.3.2.1.5 Modifiable DLT

DLT systems that allow modifications can be built. For example, the code of a blockchain used to store bookkeeping records could foresee that all entries will be purged after a certain period of time.

Chameleon hashes are one tool for allowing the modification of individual entries without breaking the integrity of a blockchain. When creating the chameleon hash, a private key is set that will have the power to modify the entry without breaking the hash. The fact that an entry was modified can remain visible. It is also possible to set conditions under which a modification will be accepted. However, the possibility to remove data removes the protection against tampering. A possible example is a bookkeeping-blockchain that securely stores information for ten years and deletes it afterwards.

5.3.2.2 Other regulatory challenges

When information on a ledger infringes on personal or commercial rights or violates criminal laws, there may be laws that require the removal of personal and non-personal data from a ledger.

5.3.3 Approaches and/or recommendations

5.3.3.1 Technical recommendations regarding standardization

5.3.3.1.1 Future PKI standardization

A DLT can be viewed as a new application of PKI, one that differs from PKI use in internet mail and browser applications, which relies on the IETF PKIX profile of X.509. There is an opportunity for useful ITU-T standardization that recognizes these differences. A standardized ITU-T X.509 DLT profile could normalize expected behavior and processing of PKI-based DLT applications.

There are two specific areas of standardization needed to support interoperability and growth in DLT applications that use PKI. One area is the development of an X.509 certificate profile for DLT, a profile that specifies required cryptographic algorithms, choice alternatives for strings and time types and useful certificate extensions. A second area is the development of DLT-specific path validation processing that recognizes the proper role of expired certificates in long-lived signed and timestamped ledgers, and that result in tool behaviors that do not obstruct ledger processing.

A profile for X.509 certificates used in a DLT context should be standardized by the ITU-T, whose SG17 / Q11 received the mandate from ISO to do so. This would serve a similar purpose as the IETF PKIX profile for internet certificates and CRLs. A DLT profile could recognize the full sweep and global nature of DLTs. This profile could recognize the need to normalize national language support by the use of UTF8String (Unicode) choice alternatives in certificate distinguished names and other instances of ASN.1 type DirectoryString, replacing the common, historic use of PrintableString (US ASCII) types.

5.3.3.1.2 A framework standardization approach (for use of symmetric cryptography in DLT systems)

A cryptographic framework approach could, or, can set the standard or interchange and leave room for the accommodation of various algorithms and key lengths without altering the definitions. This framework approach has already been codified in ANSI standards and by NIST as well. In doing so, one can adjust the algorithm and key length used. This approach provides compartmentalization and attribute based access control to anything within an enterprise that is digital: physical (door locks), logical (network access), functional (.exe or .dll) and content (any embedded digital object/word, phrase, period, etc.) all enforced by quantum-resistant, tamper-evident, cryptographic processes.

5.3.3.2 Organizational and design recommendations

a) Avoid storing clear-text personal data on a blockchain, unless you have a justification for permanence;

b) Use sidechains or other private storage options for sensitive data;

c) Use Zero-knowledge proofs where possible. However, ZKPs are still under development, some demonstrate slow performance. Standards for ZKPs are being developed [b-ZKP];

d) When storing hashes of personal data:

   i. Make sure there is enough entropy in the data hashed;

   ii. Avoid combining hashed data with other data on the blockchain;

   iii. Avoid using hash-values as identifiers;

   iv. Add secret passwords to the hashed data as an additional security measure, when this seems suitable for the application. As a sole measure, this is not sufficient, since passwords that cannot be changed do not offer advanced-level security.

e) Avoid solely relying on consent in the context of personal data and blockchains;

f) Perform a data protection impact analysis (DPIA) and a risk analysis.

Examples of approaches and/or recommendations for users, regulators and solution providers have not yet been set. Self-sovereign identity and privacy coins are two examples that use DLT to provide superior levels of privacy [b-Dunphy].

5.4 Property 4: Incentive mechanism and digital assets

Users participating in blockchain governance require incentive mechanisms. Cryptocurrencies provide incentives in a quantitative manner. Leveraging qualitative or non-financial incentives in public blockchains is also possible. However, permissioned DLTs are regarded as adept at aligning non-financial incentives with participants' objectives.

5.4.1 Introduction of the property

Incentivization directly influences governance. There is a direct correlation between creating effective mechanisms for incentive stimulations and the effectiveness of governance and vice versa. Currently, the most effective incentivization for permissionless DLTs is economic stimulation. Only when economic incentives are embedded in a system's foundation can truly complex structures be built.

These incentives are generally in a tokenized format. These tokens are limited in number and can be transferred. Within the DLT context, the concept of tokens involves technical, legal and economic aspects. In order to build a global concept valid in any jurisdiction, several legal perspectives can be adopted as either public-law (financial system) or private-law (private contracting).

Besides the native tokens, tokens can also be created by smart contracts running on a blockchain. On Ethereum, there are standards for tokens like the ERC20 for providing compatibility with wallets [b-ERC20].

The creation of tokens is called a Token Generation Event, or TGE. The initial sale of tokens is called an Initial Coin Offering, or ICO.

The Swiss regulatory authority, FINMA, classifies tokens into three categories [b-FINMA]:

- When the tokens do not prescribe any right, but can be traded, they are considered cryptocurrencies;
- When the tokens can be used as vouchers for some service on the chain or external to the chain, the tokens are considered utility tokens;
- When the tokens refer to an asset, they are considered asset tokens.

It is to be noted, for an optimal global token regulation, that the term "tokenization" usually refers to the change of system utilized for the representation of such economic valuable rights. This paper does not discuss the complex regulatory needs derived from token taxonomy or "tokenomics".

Tokenized value units of account (coin-based tokens) should be regulated by central banks in terms of national or regional monetary policy to properly control macro-magnitudes.

Additionally, a token can fall into multiple categories at the same time. Asset tokens are always treated as securities whereas utility tokens are only classified as securities in case of only having an investment purpose at the point of issue.

Compared to Switzerland, in the US, the scope of securities is broader. For example, the Securities Exchange Commission (SEC) applies the Howey-test to classify tokens as securities [b-SEC]. Regulatory oversight differs from one jurisdiction to the next and is subject to change.

Representation of rights incorporated into tokens (securities, utilities or hybrid) is the substantial issue to be addressed by legislators as it concerns the system of creation of credits (ICOs, exchange offerings, security token offerings (STOs), off-chain IPOs or service non-financial contract in the case of utilities), their cession and their extinction.

When tokens are connected to some assets, a new law is required to ensure that buyers that acquire a token in good faith are protected even when some prior transfer of the token was not carried out by the authorized token holder. New laws in Gibraltar, Liechtenstein, Malta and Switzerland have been enacted and are proposed to regulate the acquisition of tokenized assets including the actors involved [b-GFSC, b-Liecht., b-Malta-a, b-Malta-b, b-Malta-c, b-Swiss].

These legal regimes are a consequence of the "virtual incorporation" of rights occurred in an ICO or any other form of “tokenization” (i.e., constitution of rights by tokens, since they become hashed, unique and permanently sequenced units of value).

The regimes for the cession or transmission of the rights incorporated to the tokens may vary in accordance with two main factors: self-regulatory approach in an ICO or other form of issuing and legal boundaries set by deontic or imperative rules in each concerned jurisdiction, mainly investor protection applicable rules, which ICOs or token issuers must respect for reasons of public order.

However, the scope of incentive mechanisms also can include non-financial value exchanges. This supports rewards for social impact and motivation for improving or enhancing the efficiency of the DLT; the participation of the governance itself. The incentive mechanism can be also used to promote a responsible attitude in a community such as in a smart city.

5.4.2 Regulatory challenges

For the financing of blockchain projects, in addition to the conventional equity financing methods, currently, there are ICOs for utility tokens and STOs for asset and security tokens. Different countries have different policies for token-based financing methods:

- A complete ban;
- Regulation as done with securities (viewing digital objects as digital assets);
- Specialized simplified regulation;
- No regulation for pure utility tokens.

The regulators should efficiently combine different self-organizing, public-administrative and private national and international law approaches to regulate:

a) The basic blockchain, including consensus processing;
b) The smart contract validity, effects and definitions for legal purposes within the context of contract laws in different jurisdictions;
c) The optimal regimes to regulate the action of intermediaries such as the exchanges used for the fulfilment of transactions;
d) The private-law asset or security market and related public-law regimes connected to the tokens including ICOs and similar regimes.

5.4.3 Approaches and/or recommendations - Interoperability

Interoperability is defined as the "ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged" [b-ISO/IEC 17788].

Interoperability can happen at different levels. For instance, the European Interoperability Framework (EIF) [b-EIF], a commonly agreed approach to the delivery of European public services in an interoperable manner, defines a model with four layers of interoperability: legal, organizational, semantic and technical; a cross-cutting component of the four layers, ‘integrated public service governance’ and a background layer, ‘interoperability governance’.

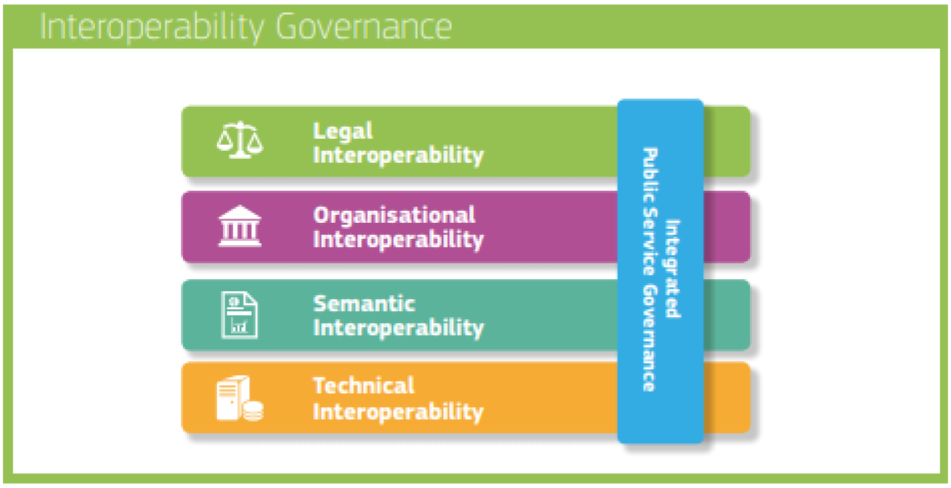
Interoperability Governance
Legal Interoperability
Organisational Interoperability
Semantic Interoperability
Technical Interoperability
Integrated Public Service Governance

Figure 1 – EIF model

Regarding technical interoperability, it may also be achieved at different levels, i.e., access, network, transport, session or application. Within the internet framework, the TCP/IP protocol has long been a basis for interoperability at network layer.

Implementations of DLT now comprise a new representation of value known as tokens or digital currency. There is a uniform approach to cross-chain interoperability described in clause 7.2 of Recommendation ITU-T X.1255 [b-ITU-T X.1255]. This "Digital Entity Interface Protocol" establishes a basis for understanding and specifying how computational operations should perform the transit, processing and storage of information across jurisdictional boundaries.

DLT can be a tool for establishing a decentralized governance that supports the attainment of the Sustainable Development Goals (SDGs). Participants who play by the rules can receive incentives whereas participants who break the rules can be punished.

Taking into account the framework, context, application and/or use case, appropriate consideration should be given to develop interoperability specifications at the right level(s) where appropriate.

5.5 Property 5: Openness, transparency and anonymity

5.5.1 Introduction of the property

Several key properties featured in DLT platforms have been long considered key for many different cases even before the creation of these technologies. The possibility of increasing transparency and, at the same time, trust, privacy and free access to processes has been a continuous quest for governments and companies alike.

The debate regarding the level of openness and transparency from DLTs should start at the discussion on permissioned and permissionless ledgers where permission refers to how the system works with respect to validating transactions. In permissioned DLTs, all the decision-making processes are derived from a trusted third party (TTP) that has exclusive roles among the network players, especially granting them access to its content and assigning the aforementioned permissions to each new player. This implies that the TTP has some knowledge about the peers.

On the other hand, on permissionless DLTs, all the peers can act freely; entering or leaving the network at any given time without identifying or authenticating themselves in a formal sense. The leaving or joining of peers does not cause any disruption unless the number of participants falls below a certain threshold. Most systems do not offer any confidentiality. Privacy, if desired, needs to be established by privacy-enhancing technology on top of the basic data layer. Some privacy coins, however, have already integrated a privacy layer for token transactions. Public DLTs do not require a permission to read blocks. Depending on the consensus algorithm used, a certain amount of computing power or a certain stake might be needed to participate in block production. Most DLT systems require some permission to write transactions, e.g. by paying with native tokens. Some countries require exchanges and wallet services to identify their customers. This information, together with the transaction on the ledger and the tracking of the IP-address where a transaction originally came from, often makes it possible to identify people using e.g. Bitcoin or Ethereum.

Permissionless DLTs are public platforms, thus they are open and transparent in essence. The sum of their features allows them to be trustless networks in which anyone could participate and independently verify the information written on the ledger, even if the parties do not know each other. Permissioned DLTs, in turn, will vary a great deal in relation to the level of openness and transparency, since they will be directly determined by the governance of the platform, which is established by a central party to a certain degree.

5.5.2 The concepts

Broadly speaking, transparency is generally associated with openness and visibility, or the opposite of secrecy. Notwithstanding, this “narrow” view of transparency fails to address some nuanced relations, as for normative dimensions. Transparency cannot simply imply revealing information anymore. It should somehow address some, if not all, of these reflexive questions in order to deal with usage, legitimacy, respect to privacy, accountability, as well as data integrity.

In that sense, in pursuit of theses normative dimensions, a modern concept of transparency could be found in ISO 16759:2013, which states transparency as “open, comprehensive, accessible, clear and understandable presentation of information”.

Regarding anonymity, currently, the ISO/IEC 20008 standard is working to describe two mechanism categories for anonymous digital signatures. One category of mechanisms for verifying signatures using a single group public key and another for verifying signatures using a set of public keys. The first mechanism category is referred to as group signatures, and the second as ring signatures. When used with blockchain technology, group signatures are more suitable for use in private or permissioned environments. Ring signatures are more suitable for use in public or permissionless environments.

Another approach to this technical challenge is the use of zero-knowledge proofs (ZKPs). Their use allows two different actors, the "proof provider" and the "verifier" to exchange the ownership of a piece of data without actually revealing the data. ZKP technologies are useful to allow the verifier to prove the ownership of a credential to the proof provider 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.

Challenges to the broad application of ZKPs (discussed in 5.3, above) are:

- They can be slow and expensive for proof providers to process. Although this issue is being mitigated by the "sapling" upgrade.
- Some identity solutions use ZKPs based on graph isomorphisms and these are faster in comparison with other ZKP variants.
- Questions remain regarding the interoperability of ZKP-based credential exchanges. While there are many ZKP variants with a wide range of performance characteristics, they are still to be considered as being in the early stages of development.

Presently, standards for a universal applicability of zero-knowledge proofs across implementations are starting to be developed [b-ZKP].

5.5.3 Regulatory challenges

Even though openness and transparency are often regarded as major positive features from DLTs, enabling them to be more trustworthy and secure, both qualities pose some challenges in certain circumstances. Distributed ledger platforms generally work on an alleged "paradox", in which, while the information on the ledger is transparent for everyone to see or read, it is also private, thus ensuring the anonymity of the players involved in a given transaction.

The balance between transparency and privacy is paramount for DLTs to comply with norms and regulations. For instance, the recent European directive in data privacy, the General Data Protection Regulation (GDPR), has the objective of conferring to the individual control of their own personal data, therefore not allowing it to be fully transparent and open to everyone. On the other hand, high levels of privacy and reduced levels of transparency are a sensitive issue for auditing and security entities that are generally concerned with the possibility of having DLT applications used for illicit activities such as tax evasion, money laundering and funding of criminal activities.

In relation to DLT, using privacy-enhancing technology, like cryptography, to design privacy almost necessarily creates a specific challenge. In other systems, an intermediary that controls access to the information has no technical restraints in providing access to the information and in deciding when to delete it. Using privacy-enhancing technology generates frictions whenever compliance requirements change or require a differentiation of disclosure of the information.

Complete transparency also poses challenges to some sectors due to their business model. The financial services sector is an example in which full transparency would not be feasible. In a transparent DLT platform, all information would be disclosed to the public such as the players involved, the pricing and the timing of the transactions along with other relevant information that would reveal much of the investment strategies of the institutions or people involved in the process. Such a level of disclosure would probably greatly affect the competitive advantage that some institutions have over their competitors.

5.5.4 Approaches and/or recommendations

Despite the general agreement on the positive impact that openness and transparency often offer, as seen before, they might also pose some challenges for certain sectors. In this sense, it is recommended that each DLT protocol and governance adjust its level of openness and transparency in accordance with two major factors:

- Regulation: Currently, many countries are reorganizing or developing their legislations to create codes to govern issues such as privacy, data management and other areas related to the internet but also new applications like cryptocurrencies. DLT platforms take into account such regulations to be able to comply with their directives;
- Sector: Each sector has its particularities. The financial sector has different demands and requirements as compared to the education or the health sectors. An efficient solution requires an appropriate DLT platform and a well-designed application.

This is further complicated by transparency and privacy requirements that change with time or relate only to certain groups. One approach often used is to store the information itself off-chain on a private storage that is access-controlled and can be deleted. On-chain solutions would only contain some hash or ZKP that enables the validation of that information. Once the original information, off-chain, is deleted, the remaining validation information should be useless. It is not possible to identify persons with this remaining validation information hence, it should not be regarded as personal data although some legal uncertainty remains [b-EU Blockchain, b-Erbguth-b].

Encrypting information on-chain is not usually recommended. Since the information is immutable, this encryption equals access control with a password that cannot be changed.

While DLTs show less flexibility in managing transparency and privacy, they also protect privacy as well as transparency against attacks from insiders and when firewalls are breached. Privacy-enhancing technology allows the uniform validation of information that is stored in different places under different access regimes. This strengthens privacy and transparency. At the same time, DLTs, as any emerging technology, are often subjected to a certain degree of distrust and doubt and their benefits and risks are not properly addressed. Adequate regulations can create incentives for innovation, which could foster superior privacy and transparency.

6 Summary

Both DLT-related opportunities and challenges, including legislative and regulatory issues, stem from the same source and result from the same characteristic of DLT properties. DLT is just a tool which is intrinsically neutral but it can be used both for good and illicit activities and the key issue is to find proper ecological niches for this technology.

The process of adapting legislation and regulations to the specific features of DLT solutions is already ongoing in many countries and it seems that nothing disruptive is required for this. First and foremost, the legislators establish the validity of transactions underpinned by DLT, such as smart contracts, cannot be denied solely because DLT was involved (the legal acceptance of digital signatures started this way as well). When traditional regulatory approaches do not work (for example, due to the absence of an official owner or controller of a solution), the legislators and regulators shift the responsibility to the persons they can apprehend thereby placing it, for example, on the end users. At the same time, the developers of DLT solutions will have to take into account the requirements of modern legislation in order to avoid being banned. As a result, it will be a mutual movement towards each other; by legislators and regulators on the one hand and system developers on the other.

The future of DLT is in seamless integration with already existing socio-political and legal systems rather than in confrontation with governments and their control. This future can be ensured by finding and filling the niches where distributed solutions and models are natural and superior to traditional solutions such as in the Internet of Things (IoT). This future includes hybrid solutions including DLT blocks being used as components of wider centralized solutions and systems.

It is not always clear how to resolve the contradiction between the immutability of the distributed ledgers and the requirements of legislation (not only privacy protection legislation which became a common boogeyman but also “ordinary” commercial law). For example, data retention and legal discovery process may require changes.

Potentially, the scope of the application of DLT solutions can include areas where cooperation between a number of “unfriendly” countries or organizations is, however, mutually beneficial for them. These parties may be hostile to each other or unwilling to publicly sacrifice even a tiniest part of their sovereignty so they cannot engage with each other through traditional channels. They can, however, accept a solution that does not have an obvious owner and allows each side to “save its face”.

Bibliography

[b-Alastria] Alastria (2019). *Inter-National Blockchain Ecosystem*. Available at: www.paymentpathways.com/wp-content/uploads/2019/01/2019JAN15-Alastria-ITU-Presentation-Rio-de-Janiero.pptx

[b-Anderson] Anderson, R., Shumailov, I. & Ahmed, M. (2018). *Making Bitcoin Legal*, 26th International Workshop, Cambridge, UK, Revised Selected Papers. 10.1007/978-3-030-03251-7_29. Available at: https://www.researchgate.net/publication/329147152_Making_Bitcoin_Legal_26th_International_Workshop_Cambridge_UK_March_19-21_2018_Revised_Selected_Papers

[b-Armstrong] Armstrong, J. (2018). *Blockchain Technology: Antitrust Risks and Safeguards*. Available at: https://mcdonaldhopkins.com/wapi/Pdf/View?url=https://mcdonaldhopkins.com/Insights/Blog/Business-Insights/2018/09/19/Blockchain-technology-Antitrust-risks-and-safeguards

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

[b-Auer] Auer, R. (2019). *Beyond The Doomsday Economics of "Proof-Of-Work" in Cryptocurrencies*. Bank of International Settlements (BIS) Working Papers, No. 765. Available at: https://www.bis.org/publ/work765.htm

[b-Austria] Austria (2018). *Federal Act concerning the Protection of Personal Data (Datenschutzgesetz - DSG).* Available at: https://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.html

[b-Baars] Baars, D. (2016). *Towards Self-Sovereign Identity using Blockchain Technology*. University of Twente. Available at: http://essay.utwente.nl/71274/1/Baars_MA_BMS

[b-Barker] Barker, E. (2016). *Recommendation for Key Management Part 1: General*. NIST Special Publication 800-57 Part 1 Revision 4. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

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

[b-Bundes Block] Blockchain Bundesverband (2018). *New Position Paper: Self-Sovereign Identity Defined*. Available at: https://bundesblock.de/de/new-position-paper-self-sovereign-identity-defined/

[b-Cutler] Cutler, J., Hansen, J. D. & Ho, C (2017). *Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues*. Perkins Coie LLP. Available at: https://www.virtualcurrencyreport.com/wp-content/uploads/sites/13/2017/05/Perki ns-Coie-Self-Sovereign-Identity-and-Distributed-Ledger-Technology_Framing-the-Legal -Issues-1.pdf [b-CNIL] CNIL (2018). *Premiers Elements D'analyse de la CNIL Blockchain*. Available at : https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf.

[b-Diaz] Diaz, J., Arroyo, D. & Rodriguez, F., B. (2014). *New X.509-Based Mechanisms for Fair Anonymity Management*. Computers & Security, Vol. 46, pp. 111-125. Available at: https://www.sciencedirect.com/science/article/pii/S0167404814001023

[b-Dunphy] Dunphy, P. & Patitcolas F. (2018). *A First Look at Identity Management Schemes on the Blockchain*. Available at: https://arxiv.org/abs/1801.03294.

[b-EDRi] European Digital Rights (2017). *Killing Parody, Killing Memes, Killing the Internet?* Available at: https://medium.com/eu-copyright-reform/killing-parody-killing-memes-killing-the-internet-b864df222047

[b-EIF] European Commission (2017). *The New European Interoperability Framework*. Available at: https://ec.europa.eu/isa2/eif_en

[b-Erbguth-a] Erbguth, J. & Fasching, G. (2017). *WeristVerantwortlichereiner Bitcoin-Transaktion? (Who is the controller of a Bitcoin transaction?)*. Zilkens: Datenschutz im kommunalenStraßenverkehrswesen (Journal of Privacy), Vol. 560. Available at: https://erbguth.ch/ZD12-2017.pdf.

[b-Erbguth-b] Erbguth, J. (2019). *Blockchain und DSGVO (Blockchain and DSGVO)*, Jusletter IT. Available at: https://jusletter-it.weblaw.ch/issues/2019/IRIS/blockchain-und-dsgvo_ea104cc327.html.

[b-ERC20] The Ethereum Wiki (2018) *ERC20 Token Standard*. Available at: https://theethereum.wiki/w/index.php/ERC20_Token_Standard

[b-EU-a] European Parliament (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[b-EU-b] European Parliament (2000). *Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of such Data*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32001R0045

[b-EU-c] European Parliament (2003). *Judgment of the European Court of Justice, C-101/01*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62001CJ0101&from=EN

[b-EU Blockchain] European Blockchain Observatory and Forum (2018). *Blockchain and the GDPR*. Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf;

[b-Evans] Evans, C., Palmer, C. & Sleevi, R. (2015). *RFC 7469 - Public Key Pinning Extension for HTTP*. Available at: https://tools.ietf.org/html/rfc7469

[b-Finck] Finck, M. (2019). *Smart contracts as a Form of Solely Automated Processing under the GDPR*. Max Planck Institute for Innovation and Competition Research Paper no. 19-01. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3311370##

[b-FINMA] FINMA (2018). *Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs).* Available at: https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en.

[b-FINRA] FINRA (2017). *Distributed Ledger Technology: Implications of Blockchain for the Securities Industry*. Available at: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

[b-DLT D1.1] ITU-T Technical Specification FG DLT D1.1 (2019), *DLT terms and definitions.*

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

[b-Grassi] Grassi P., Fenton, J., Newton, E., Perlner, R., et al. (2017). *Digital Identity Guidelines Authentication and Lifecycle Management*. NIST Special Publication 800-63B. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[b-Griffin-a] Griffin, P. H. (2018) *An Internet of Block Things*. ITU Journal: ICT Discoveries, Vol. 1, No. 2. Available at: https://www.itu.int/en/journal/002/Pages/01.aspx

[b-Griffin-b] Griffin, P. H. (2019). *Anonymous Digital Signatures*. Available at: https://mydigitalpublication.com/publication/?i=572762&article_id=3335313&view=articleBrowser&ver=html5#{"issue_id":572762,"view":"articleBrowser","article_id":"3335313"}

[b-Grover] Grover, L. K. (1996). *A Fast Quantum Mechanical Algorithm for Database Search*. Available at: https://arxiv.org/abs/quant-ph/9605043

[b-Hassan] Hassan, S. & De Filippi, P. (2017). *The Expansion of Algorithmic Governance: From Code is Law to Law is Code.* Field Actions Science Reports: The Journal of Field Actions. Special issue 17: Artificial Intelligence and Robotics in the City. Open Edition Journals. Available at: https://ssrn.com/abstract=3117630

[b-Ibáñez-a] Ibáñez, J. & Wenceslao, J. (2018). *Derecho de Blockchain y de la Tecnología de Registros Distribuidos*. Cizur Menor (Navarra): Aranzadi.

[b-Ibáñez-b] Ibáñez, J. & Wenceslao, J. (2018). *Blockchain: Primeras Cuestiones en el Ordenamiento Español.* Dykinson, Madrid.

[b-ISO/IEC 20008] ISO/IEC 20008 (2013) *Information technology -- Security techniques -- Anonymous digital signatures*. Available at: https://www.iso.org/standard/56916.html

[b-ISO 16759:2013] ISO 16759:2013 (2018). *Graphic Technology -- Quantification and Communication for Calculating The Carbon Footprint of Print Media Products*. Available at: https://www.iso.org/standard/57615.html

[b-ISO/IEC 17788] ISO/IEC 17788 (2014) *Information Technology -- Cloud Computing -- Overview and Vocabulary*. Available at: https://www.iso.org/standard/60544.html

[b-ISO/IEC 11770-2] ISO/IEC 11770-2 (2018). *IT Security techniques -- Key management -- Part 2: Mechanisms using Symmetric Techniques*. Available at: https://www.iso.org/standard/73207.html

[b-ISO/IEC 30141] ISO/IEC 30141 (2018). *Internet of Things (IoT) -- Reference Architecture*. Available at: https://www.iso.org/standard/65695.html

[b-ITU-T X.509] ITU-T X-series Recommendations – X.509 (2016). *Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks*. Available at: https://www.itu.int/rec/T-REC-X.509-201610-I/en

[b-ITU-T X.1255] ITU-T X-series Recommendations - X.1255 (2013). *Framework for Discovery of Identity Management Information*. Available at: https://www.itu.int/rec/T-REC-X.1255-201309-I

[b-Kosba] Kosba, A., Miller, A., Shi, E., Wen, Z., et al. (2015). *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts, Tech.* 2016 IEEE Symposium on Security and Privacy (SP). Available at: https://ieeexplore.ieee.org/document/7546538

[b-Larus] Larus, J. & Hankin, C. (2018) *Regulating Automated Decision Making*. Communications of the ACM, Vol. 61 No. 8, pp. 5.

[b-Laurie] Laurie, B., Langley, A. & Kasper, E. (2013). *RFC 6962 - Certificate Transparency*. Available at: https://tools.ietf.org/html/rfc6962

[b-Lessig-a] Lessig, L. (1999). *Code: And Other Law In Cyberspace*. Basic Books Inc., New York

[b-Lessig-b] Lessig, L. (2000). *Code is Law: On Liberty in Cyberspace*. Harvard Magazine, January-February, pp. 1–2, 2000.

[b-Liecht] Ministry for General Government Affairs and Finance (2018) *Government Consultation Report on The Creation of A Law on Transaction Systems Based on Trustworthy Technologies (TT) (Blockchain Law; TT-ACT; VTG) and The Amendment of Other Law*. Available at: https://erbguth.ch/2018-10-05-Unofficial-Translation-of-the-Draft-Blockchain-Act.pdf [b-Lyons] Lyons, P. & Kahn, R. (2018). *Blocks as Digital Entities: A Standards Perspective*. Available at: https://content.iospress.com/articles/information-services-and-use/isu180021

[b-Malta-a] Malta (2018). *Malta Digital Innovation Authority Act (‘MDIA’)*. Available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29080&l=1

[b-Malta-b] Malta (2018). *The Innovative Technology Arrangements and Services Act (‘ITAS Act’).* Available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29078&l=1

[b-Malta-c] Malta (2018). *The Virtual Financial Assets Act (‘VFAA’).* Available at: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lp&itemid=29079&l=1

[b-McMullen] McMullen, G. & Jongerius, S. (2018). *Privacy and GDPR Compliance of Least Authority's Private Periodic Payment Protocol (P4) Using Zcash.* Available at: https://techgdpr.com/wp-content/uploads/2019/01/TechGDPR-assessment-of-Zcash-using-Least-Authority-P4.pdf.

[b-OECD] OECD (2018). *Blockchain Technology and Competition Policy*. Available at: https://www.oecd.org/competition/blockchain-and-competition-policy.htm

[b-Peterson] Peterson, J. (2016). *Code is Law, Except when it isn't.* The Augur Report, 30-Jun-2016. Available at: https://web.archive.org/web/20170228200009/http://blog.augur.net/code-is-law/

[b-Raskin] Raskin, M. (2017). *The Law and Legality of Smart Contracts*. Georgetown Law Technology Review, Vol. 1, No. 2, pp. 305-341. Available at: https://dx.doi.org/10.2139/ssrn.2842258

[b-Rauchs] Rauchs, M., Glidden, A., Gordon, B., Pieters, G., et al. (2018). *Distributed Ledger Technology Systems A Conceptual Framework.* University of Cambridge. Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf

[b-Raval] Raval S. (2016) *Decentralized Applications Harnessing Bitcoin's Blockchain Technology*. O'Reilly Media.

[b-Reyes] Reyes, C. (2016). *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*. Villanova Law Review, Vol. 61, No. 1. Stetson University College of Law, Research Paper No. 2016-8. Available at: https://ssrn.com/abstract=2766705

[b-Russian Fed.-a] The Russian Federation (2006). *Federal Law No. 149-FZ of Information, Informational Technologies and the Protection of Information – Article 10.4*

& 10.5. Available at: https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru126en.pdf

[b-Russian Fed.-b] The Russian Federation (2017). *Contract and Obligations Law (General Part): Article-By-Article Comment To Articles 307 - 453 of the Civil Code of the Russian Federation*. rep. ed. A.G. Karapetov. M., M-Logos, pp. 708-711.

[b-Saveliev-a] Saveliev A. I. (2015). *Criteria for the Availability of Valid and Perceived Knowledge as A Condition for Holding the Information Broker to Account.* Law, No. 11, pp. 49-52.

[b-Saveliev-b] Saveliev A. I. (2016). *Elektronnaya Kommertsiya v Rossii i za Rubezhom: Pravovoe Regulirovanie [E-Commerce in Russia and Abroad: Legal Regulation]*. Moscow: Statut Publ., 640 p.

[b-Savelyev] Savelyev, A. (2016). *Contract Law 2.0: «Smart» Contracts As the Beginning of the End of Classic Contract Law*. Higher School of Economics Research Paper No. WP BRP 71/ LAW/2016. Available at: https://dx.doi.org/10.2139/ssrn.2885241

[b-SEC] SEC (2019). *Framework for "Investment Contract" Analysis of Digital Assets*. Available at: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets

[b-Sidorenko] Sidorenko E., Saveliev, A., Pushkov, A., Yankovsky, R., Chuburkov, A., Dedova, E., Gulyaeva, N., Arkhipov, V., Tyulkanov, A., Bulgakov, I., Kostyra, A. (2018). *Нужно ли регулировать биткоин? (Is it necessary to regulate bitcoin?)* SPS "Consultant Plus"

[b-Swiss] The Swiss Federal Council (2019). *Federal Council Initiates Consultation on Improving Framework Conditions for Blockchain/DLT*. Available at: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-74420.html

[b-Wack] Wack, J. (2016). *Introducing CKM Framework*. Available at: https://www.paymentpathways.com/wp-content/uploads/2019/07/2019JUL17-CKM-Framework-Description-for-Sub-group-IV-Appendix-I.docx

[b-Yaga] Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2018). *Blockchain Technology Overview*. NISTIR 8202. Available at: https://doi.org/10.6028/NIST.IR.8202

[b-Zhao] Zhao, W. (2018). *China's Supreme Court Recognizes Blockchain Evidence as Legally Binding*. Available at: https://www.coindesk.com/chinas-supreme-court-recognizes-blockchain-evidence-as-legally-binding

[b-Zetzsche] Zetzsche, D. A., Buckley, R.P. & Arner, D. W. (2017). *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*. University of Illinois Law Review, 2017-2018, Forthcoming; University of Luxembourg Law Working Paper No. 007/2017; Center for Business & Corporate Law (CBC) Working Paper 002/2017; University of Hong Kong Faculty of Law Research Paper No. 2017/020; UNSW Law Research Paper No. 17-52;

European Banking Institute Working Paper Series 14. Available at: http://dx.doi.org/10.2139/ssrn.3018214.

[b-ZKP] Zero Knowledge Proof Standardization. [online] Available at: https://zkproof.org/

ITU-T