|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATION****STANDARDIZATION SECTOR**STUDY PERIOD 2017-2020 | FG-AI4H-F-025-A06 |
| **ITU-T Focus Group on AI for Health** |
| **Original: English** |
| **WG(s):** | Plenary |  |
| **DOCUMENT** |
| **Source:** | FG-DLT |
| **Title:** | Updated baseline text: D4.1 - DLT regulatory framework |
| **Purpose:** | Discussion |
| **Contact:** | Alexander ChuburkovFintech AssociationRussian Federation | E-mail: chuburkovalex@gmail.com  |

|  |  |
| --- | --- |
| **Keywords:** | Distributed ledger technology; Regulatory Framework |
| **Abstract:** | This document provides an updated draft of ITU-T FG DLT D4.1 - DLT Regulatory Framework following the FG DLT meeting in Madrid, 1-4 April 2019. |

**ITU-T FG DLT Deliverable D4.1: DLT Regulatory Framework**

CONTENTS

[1 Scope 4](#_Toc535939293)

[2 References 4](#_Toc535939294)

[3 Definitions 4](#_Toc535939295)

[4 Abbreviations and acronyms 4](#_Toc535939296)

[5 Conventions 4](#_Toc535939297)

[6 Introduction 4](#_Toc535939298)

[6.1 DLT key properties 5](#_Toc535939299)

[6.2 DLT regulatory issues 5](#_Toc535939300)

[7 Property 1: Distributed fashion (i.e., without a central repository) 6](#_Toc535939301)

[7.1 Introduce the property 7](#_Toc535939302)

[7.2 Regulatory challenges 9](#_Toc535939303)

[7.3 Approaches and/or recommendations 10](#_Toc535939304)

[8 Property 2: Tamper evident and tamper resistant 11](#_Toc535939305)

[8.1 Introduce the property 11](#_Toc535939306)

[8.2 Regulatory challenges 12](#_Toc535939307)

[8.2.1 GDPR Data retention & destruction 12](#_Toc535939308)

[8.3 Approaches and/or recommendations 12](#_Toc535939309)

[9 Property 3: Shared ledger 12](#_Toc535939310)

[9.1 Introduce the property 13](#_Toc535939311)

[9.2 Regulatory challenges 13](#_Toc535939312)

[9.3 Approaches and/or recommendations 14](#_Toc535939314)

[10 Property 4: Incentive mechanism and digital assets 15](#_Toc535939315)

[10.1 Introduce the property 16](#_Toc535939316)

[10.2 Regulatory challenges 17](#_Toc535939317)

[10.3 Approaches and/or recommendations 18](#_Toc535939319)

[11 Property 5: Openness and transparency 20](#_Toc535939320)

[11.1 Introduce the property 20](#_Toc535939321)

[11.2 Regulatory challenges 20](#_Toc535939322)

[11.3 Approaches and/or recommendations 20](#_Toc535939323)

[12 Property 6: Anonymity 20](#_Toc535939324)

[12.1 Introduce the property 20](#_Toc535939325)

[12.2 Technologies for strong anonymity 20](#_Toc535939326)

[12.3 Regulatory challenges 21](#_Toc535939328)

[12.4 Approaches and/or recommendations 22](#_Toc535939329)

[12.5 References 23](#_Toc535939330)

[13 Property 7: Autonomy 23](#_Toc535939331)

[13.1 Introduce the property 23](#_Toc535939332)

[13.2 Regulatory challenges 24](#_Toc535939333)

[13.3 Approaches and/or recommendations 25](#_Toc535939334)

[14 Summary 26](#_Toc535939335)

[**Appendix I** Security issues in DLT (Hierarchical PKI assymmetric cryptography issues) & (Peer-to-Peer CKM symmetric cryptography issues) 30](#_Toc535939336)

[**Bibliography** 31](#_Toc535939337)

ITU-T FG DLT Deliverable D4.1

DLT Regulatory Framework

# Scope

This document contains a DLT Regulatory Framework. This document identifies key properties of DLT as well as associated regulatory challenges. The document then develops approaches and recommendations for users and regulators for overcoming these challenges.

# References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this document.

# Definitions

This document applies the terms and definitions defined in ITU-T FG DLT D1.1.

# Abbreviations and acronyms

This Document uses the following abbreviations:

DLT Distributed Ledger Technology

PII Personally Identifiable Information

*[to be completed]*

# Conventions

This clause is intentionally left blank.

# Introduction

Many groups are developing frameworks featuring DLT. This paper considers the key properties of DLT that are common among the diversity of these approaches. By exploring potential issues that can arise with their use, we hope to raise interest in further investigation and bring into focus topics of concern to Regulators. Additionally, by supplying practical recommendations for users, regulators, and technologists, we hope to mitigate risks of potential harms.



The document is organized in chapters that correspond to the essential features of the DLT. Each chapter describes specific problems and risks as formulated and assessed by experts. Each chapter addresses these risks in the form of recommendations for users, regulators and technologists. Each Chapter contains bibliographic links. This [Link](http://www.paymentpathways.com/wp-content/uploads/2019/01/2019JAN15-Alastria-ITU-Presentation-Rio-de-Janiero.pdf) retrieves the Alastria presentation.

## Summary of key DLT properties

Distributed fashion

Tamper evident and tamper resistant

Shared ledger

Incentive mechanisms and digital assets

Openness and transparency

Anonymity

Autonomy

Governance issues are central to our work. We mark regulatory issues that could arise in early adopter Use Case implementations of DLT. For example, there are properties of digital entities (aka digital objects) that are crucial to legal enforcement of rules such as Liable Provenance, Intent, Attestation of accuracy, chain-of-custody, etc.

Public DLT may fall down if put into practice without a framework that functions to measure, assess, and enforce. For instance, governance might perform the duty of verifying log entries are current, accurate and adhere to rules requiring completeness. Sloppy management of an access control list could open rather than restrain access to and usage of data stored in a public blockchain.

A gap could exist if rules do not require an enforcement mechanism for intervention or revocation of privilege to protect against further misuse of privilege and remediate any potential harm that does occur.

Increasingly, Use Cases have a plethora of machine-to-machine transactions driven by smart contracts that run as a user with ‘permissions.’ Humans don’t have the ability to audit every single line of source code in modern day computing devices. Humans, acting as agents of corporations, bear responsibilities for process outcomes that software only does what specifications claim it does. Regulations prescribe what amount of testing is required to meet threshold requirements of fault-isolation / fault-tolerance / suspicious activity reporting, etc.

## DLT regulatory issues

The following table lists some key publication sources that deal with DLT’s regulatory issues:

Table 1: DLT features and regulation challenges

|  |  |
| --- | --- |
| DLT features | Regulation challenges |
| **Distributed fashion** (i.e., without a central repository) [NISTIR8202, ii, Abstract, 3] | 1) territoriality of applicable law with respect to multiple nodes established in multiple jurisdictions;2) who will be legal subject;3) distributed storage solution needs to be developed in order to meet the requirements of production environments.4) Interoperability requirements;5) New models of business process, trading and organizations; |
| **Tamper evident and tamper resistant** [NISTIR8202, 7.1, Immutability] | 1) immutable shared ledgers, error corrections mechanisms2) right to be forgotten3) smart contracts |
| **Shared ledger** | Privacy & data protection*In a DLT network, data (including certain customer information and transaction records) may be shared by all parties on the network. Even where such data is encrypted, it may be vulnerable to being exposed or accessed by undesired parties on the network* [FINRA, «Distributed Ledger Technology: Implications of Blockchain for the Securities Industry», 16]How to protect user data (password…) in open environment?How to mitigate risk of data abuse in open environment?The security issue of blockchain system includes 'Smart Contracts,’ not only on-chain data protection. |
| **Incentive mechanism and digital assets**[NISTIR8202, 54][FINRA, «Distributed Ledger Technology: Implications of Blockchain for the Securities Industry», 3]  | 1) *What is token/coin?* (the definition of ‘token’ is unsettled and may depend on legal jurisdiction. reference FG-DLT taxonomy for definition)2) *What kind of ICO is legal?* 3) *What’s the next crypto-economy system, not only the current token economy?*4) *A DLT network designed to facilitate securities transactions may present new and unique challenges related to maintaining appropriate supervisory policies and procedures and surveillance systems in accordance with applicable rules* (e.g.,FINRA Rules 3110 and 3120). *For example, FINRA’s supervisory rules require the review of customer account activity as well as the review of post-trade transactions, such as account designation changes, to correct order errors* [FINRA, «Distributed Ledger Technology: Implications of Blockchain for the Securities Industry», 18] |
| **Openness and Transparency**[FINRA, «Distributed Ledger Technology: Implications of Blockchain for the Securities Industry», 6,10] | Abuse, e.g., financial crime, abuse images, dark web links, Wikileaks, personal security… |
| **Anonymity**  | 1) No-name users (including obfuscated and/or encrypted digitalized abstracted ‘names’ (or ‘handles’) vs. identification (AML/KYC) |
| **Autonomy**  | 1) You cannot stop Source Code (SC) execution |

# Property 1: Distributed fashion

**Distributed fashion** *also implies operation without a central repository.*

The characteristic of the term 'distributed' in an IT context is based on something which is shared among multiple systems and which may also be in different locations. **Distributed fashion,** as mentioned at NISTIR 8202, could be aligned to a community system of layers whereby the anatomy of a DLT System is described as follows: protocol layer, orchestration layer, business layer, network layer, and data layer. For instance, concerning the Orchestration Layer – ISO/IEC 38500, ISO/IEC TR 38502, ISO/IEC 38501 – address considerations of Directives, Regulations and Jurisdictional rules.

A decentralized process should not be confused with a distributed process. When a distributed process is divided into parts and occurs across multiple servers or nodes, the process may offer efficiencies and higher resilience over using just a single node. When a process is decentralized multiple nodes are again in use but in this case, the process is managing the same storage or executing the same program as all of the others.

Decentralization in a DLT system is not a binary property. It is the accumulation of behaviours at multiple layers. A Distributed system can have different degrees of decentralization at each of its layers.

## Introduce the property

‘Distributed fashion’ permits associative models of auto-governing rules to facilitate a useful, trust-less, and efficient system. It is, in abstract, a community of layers. Simply put, the totality of layers and pillars of design principles can be decentralized whereby authority is segregated between ownership and usership. This approach intends to be symbiotic with maintenance and governance. This ‘Distributed fashion’ property encompasses: a.) All matters of concern that might exist between liable entities; b.) Allowance for the opportunity to change their protocol of governance under specific rules which legitimize this change of protocol layer. The scope of this property includes defining regulatory boundaries and gateway protocols to achieve liability isolation that is distinguished by the context of multi-lateral or bi-lateral data exchanges. Thanks to these properties, interoperability with another DLT ecosystem, can be proposed by: a.) A participant network; b.) By a data owner; or c.) By both … to change the protocol layer and adjust it on accordance with prevailing rules.

The genesis component enlivens the system by testing, using and hacking to determine some patterns. These patterns reflect the socio-political state of the world where and when they are found on-chain.

The University of Cambridge Report entitled, “DLT systems a conceptual framework” was published in August 2018. The following table, mapping a diverse array of governance models to DLT implementations, is a derivative update to that work:

Protocol Governance Configurations (Partial list)

|  |  |
| --- | --- |
| Configurations | Examples |
| Negentropic | Bitcoin |
| Autocratic | Ripple, Project X, Hyperledger.  |
| Hierarchic | Ethereum Foundation |
| Plutocratic | Alastria |
| Democratic | Democracy.earth |
| Futarchic | Aragon, Gnosis |
| Federated | Verified.me |

**Protocol Governance Models /or/ Governance Decision-Making Process Models**

|  |  |  |  |
| --- | --- | --- | --- |
| Locus of Control / Trust Model | Decision-Making Process | Meaning  | Examples |
| 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. person, company, mining pool). | 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  | PlutocraticUnequal Horizontality | Protocol change proposals are voted on, with each vote 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 DemocraticAutonomous 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 markets models are used to determine which policies will have the most positive effect | Aragon, Tezos, Gnosis |
| 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 |

**Distributed fashion** implies that at every origin event, there must be at least a constitution (Genesis component) and a governance model (Alteration component). The conflict between:

1. Having unfettered freedom to deploy and use a DLT-based framework under a peaceful association as a Human Right; versus
2. Having limitation(s) of Right(s) whereby some guidance (of rules and policies) places restraints on DLT-based framework deployment and usage activities. E.g.: *a 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.



The figure above from ISO TC307 WG1 distinguishes a five layer hierarchical framework/reference architecture of Blockchain and related distributed ledger technology.

Each of five layers and the common connective ‘cross-layer,’ have two phases:

a.) A static phase which is the Genesis phase;

b.) A dynamically growing phase which is the Alteration phase (when correction of coding errors, upgradeability, ponderation of alterations, and how alteration can be legitimatized to be implemented, etc.

The table below from the Cambridge report distinguishes three levels for altering the protocol governance layer which is, in functionality, a hierarchical critical configuration based on: 1.) Proposal; 2.) Funding approval; and 3.) Implementation.

Protocol Change Configurations

|  |  |  |
| --- | --- | --- |
| Lense | Configurations | Description |
| Proposal | Open alteration | Open systems allow anyone to propose. |
| Filtered alteration | Proposals are conditional on some requirement of the system. e.g. Dash and Tezos. |
| Authorized alteration | Corporations or consortia may restrict who can propose. |
| Funding | Altruist | Some protocols rely on volunteer efforts, like Monero, working through voluntary charitable contributions by token holders or other interested parties. |
| Supported Development | Ethereum Foundation may fund through grants. Note: this has a centralizing effect on the protocol layer. |
| Network funded development | Can be subject to approval(s) of participants in a network. e.g.: generating objectives or goals which when met, earn a ‘bounty.’ a.k.a. incentive reward. |
| Corporate sponsored development | Corporations (directly) or Consortia (indirectly) through sponsoring organization. |
| Implementation | Run client software of choice | No action from an administrator is required, but this may result in network splits from contentious or uncoordinated changes; this mode tends to reduce developer or record producer control of the governance process. |
| Pushed to clients | By pushing updates and/or upgrades by deprecation notice directly to clients, generally launching by an administrator or an on-chain governance system. This mode tends to prioritize the integrity of the network, but may tend to cede power to developers or record producers. |

Challenges associated with this property:

1. Heterogeneity: enable users to access and run applications over a heterogeneous collection of computers, devices, operating systems, programming languages, node´s managers and networks.
2. Security: Integrity, confidentiality, enforceability, availability and usage. Some constraints may work at cross-purposes and require multiple protections to satisfy criteria drawn from different governance authorities.
3. Concurrency:
4. Failure handling: Distinction between the incident management model and the incident governance model. 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 incident management model.
5. Cross-border transfer and Data localization: Collecting Data, Retaining Data, Analyzing Data, Deleting Data and Sharing Data.

## Regulatory challenges

The main disruption in technology is disruption of law. Regulatory challenges are first addressed by identification of the following pain points:

* Data Storage and Privacy & Personally Identifying Data (PID) as defined in GDPR. Note: PID and public data alike, fall under regulatory purview if derived from other non-protected, data attributes: Directives, Regulations and jurisdictional impact on personal data protection. Portability.
* Human behavior, fixed by algorithm and consensus, are creating ethical and socio-political cyberspaces based on freedom and Human Rights. For example, the [Right of Association](https://en.wikipedia.org/wiki/Freedom_of_association) affects restrictions and/or limitations, but also is an alive foundational scenario. ~~since inception.~~ “Code is law” is a recent phrase that confers meaning that the identification of the common behaviors on those associative models can be instrumental in providing an arbitration/dispute resolution result than an off-chain alternative method would be able to accomplish. But this ignores the nuance of the pragmatic world of law. For example, there is an evolution of DAO (Decentralized Autonomous Organization) to DAC (Decentralized Altruistic Community) and hybrid denominations or inter-blockchain relationships by agreements or alliances which is not easy to regulate on-chain, nevertheless a combination with off-chain governance is the sole solution in this moment under a regulatory prospective.
* Redemption: Governance of modesty (For example a check claimed (delayed payment) based on a license). Reputation of SSI, Reputation of the framework itself.
* Multi-jurisdiction and arbitration: ponderation of conflicts to be resolved automatically or autonomously and maintain the persistence of the framework and which conflicts are destined to the off-chain resolution or off-ledger solution, in this case territorially applicable law would be assume by the good will and self-sovereignty to govern ourselves as users. Otherwise, territorially applicable law would be defined by the DLT system. In both circumstances, the territorial point of data-origination or the territorial point of data-consumption would need to be established in order to determine venue (legal system / jurisdiction) and manner (process) for the remediation of harm(s).
* Market Competition: Competition Law.
* Interoperability. Consolidate a multi-framework is not only a future exercise.
* Discoverability and Copyrighting conflicts.
* Exogenous and Endogenous data and inter-rationale environment. “Rule initiation refers to defining ruleset upon which the DLT system will operate. This process can be performed by different actors” [Cambridge University report “DLT systems a conceptual framework”, August 2018](http://www.paymentpathways.com/wp-content/uploads/2018/11/2018-08-conceptualising-dlt-systems.pdf)

## Approaches and/or recommendations

Examples of approaches and/or recommendations for users, regulators and solution providers to address the challenges associated with this property are dynamically launching new challenges, however it is identified some of the following system interactions:

1. Within the System Boundaries: Guidance is an exercise of compliance to provide the information enough about the legal biding of layer interdependencies, layer hierarchy, trade-offs and decentralization.
2. Beyond the system Boundaries: Self-sufficient, Dependent System, Interfacing System, External System, Inter-System dependencies.

Mehari is a method for risk analysis and risk management developed by CLUSIF (Club de la Securite del' Information Francais). Magerit is a risk analysis and management methodology for information systems developed by CSAE (Consejo Superior de Administracion Electronica).

NIST800-30 is a risk management guide for information technology systems recommended by the National Institute of Standard and Technology (NIST) in NIST Special Publication 800-30. Microsoftpsilas Security Management Guide is a security risk management guide developed by Microsoft.

Table n: Data protection laws

|  |  |
| --- | --- |
| Jurisdiction | Law |
| Europe | [GDPR (2016).](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL) There is a first statement of the French DPA CNIL on blockchain, see <https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf>, as well as a statement from the EU blockchain observatory, see <https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf>  |
| China | Personal Information Security Specification (Standard, 2018) |
| Australia | [The Privacy Act 1988 (Cth)](https://www.oaic.gov.au/privacy-law/), which includes the Australian Privacy Principles (APPs) |
| US | [Privacy Law Ad Hoc](https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa) |
| Canada | Privacy Act (2013) and [PIPEDA (2018)](https://en.wikipedia.org/wiki/Personal_Information_Protection_and_Electronic_Documents_Act) |
| Russia | [Conglomerate of related laws](https://uk.practicallaw.thomsonreuters.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1) and OPD Law. New Data Protection Law is coming with essentials on GDPR. |
| Brazil | [LGPD (2018)](https://www.pnm.adv.br/wp-content/uploads/2018/08/Brazilian-General-Data-Protection-Law.pdf) |
| ~~UK~~ | [~~Data Protection Act 2018~~](https://www.gov.uk/government/collections/data-protection-act-2018) |
| Singapore | [PDPA (2012)](https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview) |
| India | [Personal Data Protection Bill 2018](http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018.pdf) |
| Korea (Rep. of) | PIPA, UPCIA, IT Network Act |
| Japan | APPI and other related laws |
| Switzerland | DPA currently under revision |
| South Africa | POPIA (2013) |
| Mexico | LFPDPP (2011) supplemented in 2013 |
| Cyprus | Data Protection Law (2018) supplementing GDPR |
| Vietnam | Law on Cyber Information Security (2016) |
| Malaysia  | Personal Data Protection Act 2010 (2013) |

In addition to Data Protection regulations listed above, there are related sectorial, federal, national or local laws. Depending on the jurisdiction, such laws may contain specifications and/or special rules and security considerations for consumer protection, cyber-crime mitigation and telecommunications, which support a regulatory framework for countries with no General Data Protection Regulation (GDPR) Law. For instance, in the United Arab Emirates there is a law which covers the area of Data Protection with these sectorial laws and/or Dubai International Financial Centre (DIFC) covers data protection area with DIFC Data Protection Legislation with consolidation and amendments in 2018.

# Property 2: Tamper evident and tamper resistant

# Tamper evident and tamper resistant *also implies minimizing harms caused when the collection, disclosure, and disposition of data is inconsistent with purpose and authority.*

## Introduction of the property

DLT provides a conceptual model for providing tamper resistance based on multiple duplications of a ledger among different users, who are involved in governing a DLT system. In order to tamper the data in the ledger, a malicious user must persuade multiple users to act or react according to his suggestion, which becomes more difficult as populations of users increase.

When a user’s copy of a ledger differs from the copies that other users provided, evidence of possible tampering is established. Note, that in such a case, the copy of a ledger is deemed to be broken – it is no longer valid and cannot be used any more – henceforth, the copy must be updated (corrected) or discarded.

8.1.1 Challenges associated with this property

* Assessment of the actual level of tamper resistance – due to many kinds of attacks on DLT systems aimed on tampering the data, the security of each protocol in the base DLT system should be evaluated for effectiveness and weaknesses identified.
* The need for tamper resistance assumes the storage of the ledger which is always growing. This is challenging for scalability of a DLT system.
* Regulation that requires the correction or removal of data in the ledger.

## Regulatory challenges

### GDPR – Data protection

The European General Data Protection Regulation (GDPR) applies to outside Europe in certain conditions when processing affects controller in Europe…all data processing of personal data whether or not the controllers or processors of data are located in the EU or wherever the controlling or processing of datasets that target the European market are located to access and use the data of people in Europe.

The GDPR requires a justification for any processing of personal data. Possible justifications include: data subject’s consent, performance of a contract with the data-subject, legal obligations and legitimate interest. Although people often focus on consent, consent is often not suitable in the context of blockchains because it can always be withdrawn.

The GDPR 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 is in direct conflict with the immutability of DLT systems. The right to be forgotten, however, is not limitless. It exists only under the condition that there is no more justification to store the original data.

There are five (five or four?) general ways, a blockchain’s governance authority can cope with GDPR:

1. Never store personal data on blockchains. 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 information is already considered personal data. A common way forward is to store the main data outside of a blockchain and use the blockchain for verification, ordering and time-stamping. This is done through the use of hashing the personal data. However, hashes of personal data might represent personal data themselves. See below for more details on hashing.
2. Neither operators nor Relying Parties should have: a.) control of the blockchain or b.) control of the keys for writing the subject data on the blockchain. E.g.: When a data-subject stores her personal data on a public blockchain, the French data protection authority CNIL sees the data-subject as the controller. A company that merely provides the tools to do so is not seen as being a controller and therefore not responsible for this.
3. Only store such datasets on public blockchains that are justified to be publicly accessible for a very long time. GDPR protection ends with the death of the data-subjects.
4. Use blockchains where data will be purged after a certain period of time. Chameleon hashes are one form of implementation for automation of the purge function. Permissioned blockchains where a central authority can decide to remove specific data might also be a solution in some cases. However, the possibility to remove data removes trust. Immutability of DLT-systems is not an accident that just needs to be corrected.
5. Use privacy enhancing techniques like Zero Knowledge (ZK) proofs. There is a debate whether these privacy enhancing techniques always render the data on the blockchain anonymous.

A recent decision by the Austrian data protection authority Datenschutzbehörde suggests that reasonable protection against deanonymisation should be enough.

This position is consistent with GDPR language and also suggests that a light regulatory touch would is practical and sufficient because when one assigns good cryptographic technologies, the threshold need not be higher than conventional systems.

Due to the facts that:

a.) One can never be sure of anything;

b.) Present standards are reasonable; and

c.) The same threshold should be set in blockchain.

…it is impossible to predict:

1. When data protection technologies will become obsolete;
2. When there is some risk that data on the blockchain might still be considered personal data after data access controls expire or become compromised.

The CNIL sees ZK Proofs (ZKPs) as an appropriate access control mechanism to reduce the risks to data subjects. While CNIL was not considering a case of blockchain, it is a good sign that normative data security thresholds should be regarded as sufficient. When using hashes of personal data on a blockchain, extreme care must be taken that the data on the blockchain does neither directly nor indirectly reveal information about data-subjects~~. (relocate)~~ Keeping ZKP and normative threshold policies in mind, these characteristics may require updates to maintain access control *but this should not be a reason to delay deployment of DLT technologies.*

Typical pseudonymization scenarios where only identifiers (or pointers to external repositories) are replaced by hashes (or even random numbers) are usually still considered personal data.

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 that have the 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 already known to people that are in possession of the information hashed.

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 the access to the hash, then it is called pepper.

## Approaches and/or recommendations

* Avoid storing clear text personal data on a blockchain unless you have a justification for permanence.
* Use Zero Knowledge Proofs where possible. Limitations are:
	+ They can be slow and expensive for proofers to process. While there are many ZKP variants, with a wide range of performance characteristics, they are still to be considered in early stages of development;
	+ Some identity solutions use ZKPs based on graph isomorphisms, and these are exceedingly fast in comparison with other ZKP variants; and
	+ Questions remain on the interoperability of ZKP-based credential exchanges.
	+ At this time, standards for a universal applicability of zero knowledge proofs across implementations and technology suppliers do not exist.
* When storing hashes of personal data
	+ Make sure there is enough entropy in the data hashed
	+ Avoid combining hashed data with other data on the blockchain
	+ Add secret passwords to the hashed data and use encryption for data not hashed but combined with the hash when this seems suitable for the application
* Avoid using consent in the context of personal data and blockchains.
* Using sidechains for sensitive data
* Perform a Data Protection Impact Analysis (DPIA) and a risk analysis in order to choose appropriate protocol.

Examples of approaches and/or recommendations for users, regulators and solution providers to address the challenges associated with this property have not yet been addressed and are out of scope at this time.

# Property 3: Shared ledger

**Shared ledger** *also implies a methodology for the storage and retrieval of data in a manner that protects the sequence and fidelity of stored data from any alteration whatsoever prior to its retrieval.*

## Introduce the property

Distributed Ledger Technology (a.k.a. ‘blockchain’) technology is not just a simple concept of "distributed" and "shared". It uses cryptography, distributed databases (large-scale data storage and processing), peer-to-peer communication (P2P network), consensus mechanisms and other technologies to combine innovations.

In a narrow sense, blockchain technology is a non-tamper-able and undeletable decentralized shared ledger enforced by cryptographic functions that combine data blocks in a chronological order into a specific data structure in the form of a linked list. It can be safely stored simply. Any data that has a relationship can be verified in the system. The generalized blockchain technology refers to the use of cryptographic mechanisms to verify retrieved sequenced data has perfect fidelity with sequenced data stored. This is often referred to as data integrity. It is not to be confused with data accuracy. For there to be high confidence in data accuracy, a responsible entity’s attestation of accuracy must bind to data before is written to a blockchain or DLT-based repository system. Shared ledger does not solve data accuracy protection.

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 de-centralized (multi-centered) infrastructure that is a new distributed computing paradigm that has a mechanism of enforcement that adheres to operating rules in a manner that is persistent and consistent in a variety of settings.

## Regulatory challenges

The DLT technology has the following challenges:

**- Scalability**

There are blockchains with PoS and DPoS which are extremely fast. In this context, the main problem is not performance but scalability. This also implies that relying on a single database as a tool for providing trust exposes the problems of transporting and processing huge amount of data for a single node.

**- Privacy protection**

The entire book of the blockchain is public, but what if some people/institutions do not wish to have their funds transactions be visible across the network, especially large transactions? See ZKP discussion, above.

**- Security issues**

At present, smart contracts are still in their infancy. Once there are loopholes, they will be attacked and there will be significant risks. For example, The DAO was hacked. The hacker used the security vulnerability of The DAO smart contract to remove 3.6 million ETHs from the contract management ETH.

Note regarding the security of smart contracts (or any kind of high-value data): When a PKI is used to support certificate-based signature, the certificates have a validity period and a potential to be blacklisted. A contract or other data signed on a ledger may become unreliable as to its data integrity attestation/origin authenticity if the signer certificate for that attestation has expired or has become blacklisted. This will be problematic should a high level of assurance in the data is still required and could interrupt the automatic execution of smart contracts in such circumstance.

**- Governance challenges overview**

When the community faces major decision-making events, issues that arise are: a.) How to get the community involved; b.) How to form a community opinion with a certain mechanism; and c.) How to express it on the blockchain with finality. These decisions may range from a different technical upgrade proposals to how to handle incidents such as the DAO, to making adjustments to some of the basic rules of the blockchain. In the absence of any structural governance mechanism to address problems, resolutions to problems could:

a.) Require short time to solve with subtle fixes (soft forks); or

b.) Require long time to solve (Hard forks) by incurring protracted developer/miner debates.

The mere irregularity of ensuing outcomes can lead to confusion and division.

Governance responsibilities at this early stage should not necessarily include the identification and development of mechanisms that militate cyber-security threats to datasets that are stored on blockchains and DLT. This topic is beyond the scope of this document because cyber weapons are recognized as the perfect ‘Hard Power’ weapons. They get the job done, they are cost-effective, and they are deniable.

However, there are concerns about identifying how possible ‘soft power’ leverage can be applied by entities with substantial resources to influence outcomes. Governances can and should choose to address such cases. A partial list (3) of topics, that in the opinion of the authors, require further investigation are: Anti-Trust, Continuous Audit, and Data Accessibility.

**- Anti-Trust**

Problem definition: *Anti-Trust concerns arise when a multitude of different products are produced, supported and promoted by different parties (consortia, associations and even individual organizations).*

There is evidence of a full-fledged and solid competition in the DLT platform marketplace (whereas the Internet, which has become one and universal, as a digital medium has no direct competitors as such).

This is important because DLT is a network effect technology (e.g. the value it creates increases in proportion to an accelerating number of users).

Rather than drawing comparisons of the DLT market to the Internet, it is more likely to be regarded as comparable with several markets:

a.) The market of communication services;

b.) The market of digital platforms;

c.) The market of social networks

… and other markets where many players struggle to get the strongest network effect.

This analogy also relates to the DLT market because the same consumer can be a client of several players at the same time and bring usefulness to network effects simultaneously to multiple number of such parties.

Depending on legal circumstances, there may be problems in complying with certain antitrust requirements when joining different DLTs:

- For instance, a problem may arise when there is a dominant player, unreasonably denies all or some participants from having access (or biased implementations that choose only select partners to join) - the problem of abuse of dominant position;

- Alternatively, the problem may be opposite, when individual participants, will refuse to compete with each other in separate segments, thus carrying out a kind of division of this digital market or performing other actions that restrict competition

- Thirdly, the formation of a hybrid DLT cartel can be a hybrid variant.

**- Continuous Audit**

On the one hand, the enforcement of antitrust measures applied to DLT may require identification of the circumstances when fiduciary duties would/could/should become the burden of software developers.  This view interprets DLT as being in a “Wild West” stage of life.  Liability is often not accepted by authors that ‘code’ is solely functioning within the scope of design-objectives in written specifications. Furthermore, the continual validation of Digital Objects (by designated nodes of equivalent strength) prior to writing to a shared ledger is a practice that is beneficial to regulators.

There is a need for a vetting process of the validators and opportunity under regulation for good governance and oversight principles to be set up. The need for speed of correction, erasing fake values, adding purposeful management of data such as not uploading complete profiles or data sets or bogus cleaning procedures to eliminate data, etc.

On the other hand, we need to view the role of audit from the perspective of different legal jurisdictions. There are two facets of continuous audit: a.) The digital trail of a transaction or message from the point of initiation to the point of receipt; b.) A machine or node audit for the system must know which nodes are operative or inoperative. If signalling indicates “inoperative” is the node experiencing technical difficulty or has it shut down. Fail-safe engineering principles require precision in meaning in order for information to not be misinterpreted.

If a node is down or off, an out of band notification is sent to the defined set of responsible employees.

It seems unusual but might be possible that some law in a legal jurisdiction would be opposed to continuous audit in a closed system. Should such a circumstance exist, regulators in such jurisdictions would need to reach understanding with counter-parties how and under which constitutional jurisdiction to remediate harms. Technically we could program for audit to stop at nodes where such a jurisdictional boundary may exist, but insurance coverage would also stop at that boundary.

This view interprets DLT as being in a Pre-Cambrian stage of life. Regarding liability isolation matters, perhaps a vigilant, yet light regulatory touch is appropriate in order to not impede innovation in an important technology and development that has many implications for the UN’s seventeen Sustainable Development Goals.

**- Interoperability**

The Internet has a common TCP/IP protocol as the basis for interoperability. The various kinds of DLT implementations comprise a new generation of value known as blocks. A uniform approach to cross-chain interoperability is described in clause 7.2 in [b-1255] and is known as the Digital Entity Interface Protocol.

**- Data Accessibility**

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

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

Alongside language and message standards, are Attribute-based Access Control (ABAC)[23] and Rule-based Access Control (RBAC) methods to protect data privacy and restrict data usage. Access control models provide a framework and set of boundary conditions upon which the objects, subjects, operations, and rules may be combined to generate and enforce an access control decision.

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

Data exchanges may occur between side-chain and DLT systems operations with different governance models and/or different constitutional legal systems. To remedy harms caused by a responsible party’s failure to operate data protection and/or access controls properly, *a priori* agreement which jurisdictional authority will resolve conflict issues is mandatory. Policy Enforcement Point (PEP) signify an intersection of jurisdictional boundaries where data protection and access control duties are clarified.

Entity types of “named” Digital Objects:

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

Broad-reaching language and messaging standards enable inter-operable exchange of data (including ‘named Digital Objects) across jurisdictional boundaries:

* Universal Business Language standard (ISO 19845)
* Universal Financial Industry Message Scheme (ISO 20022)

“What entities” (e.g. Token or Account based digital currencies) are the subject of an emergent standard to define how named Digital Objects at the Edge enforce data access behavior across jurisdictional boundaries.

* Security Aspects for Digital Currencies (TS 23526 under SC2) The objective of this technical specification ISO standard is to develop a framework providing attribute-based access control to self-protecting data objects indifferent to network topography or platform.
* Note: TS 23576 for Blockchain and ledger under TC307 is an ISO technical report but not a standard.

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

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

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

For example, the ITU focus on Blockchain, as a use case for digital fiat currency, has a different emphasis than the upcoming ISO 23526 standard development.  Several countries have voiced that the digital currency security ISO standard effort should not include Blockchain since it is being emphasized in a separate ISO standard effort.  It is likely that the current ISO Blockchain efforts will be cross-referenced by the ISO digital currency security effort (23526) once the digital currency security effort advances.  ISO 23526 authors are working with others in looking at ‘cash’ and ‘cash with applications’ to differentiate where anonymity and identity can have roles through security technologies. Perhaps this methodology within a digital currency context can be of use for Blockchain since there are similar separations for a closed or open Blockchain concept.

## Approaches and/or recommendations

There are six dimensions of blockchain technology shown as below:

1. From the information system perspective, DLT technology is a new database technology, jointly maintain a growing multi-distributed data recorded by cryptography technology to protect content and timing data is difficult to tamper with, deny, and delete.
2. From the perspective of the accounting, the DLT is a brand-new distributed ledger technology. Anyone who meets the rules can obtain the billing right. All the people share and share the book information, and can detect and verify the book information.
3. From the perspective of the account, the DLT account is a new kind of account system. The private key is locally generated based on the asymmetric key technology, and the public key is derived therefrom, and then the wallet address is transformed. The third party does not need to participate in the whole process of opening an account.
4. From the perspective of asset trading, this is a brand-new value exchange technology that supports both UTXO and account models. By Mapping and reducing, UTXO can be converted into account balance, and splitting the account balance can get UTXO results. Based on this value exchange technology, we can create a new financial market model: decentralized asset trading。
5. From the perspective of organizational behavior, it is a new type of de-organized distributed collaborative production activity. It clarifies the economic interests of all parties by stimulating compatible algorithm rules and contractual arrangements, and fully mobilizes all parties. The enthusiasm makes effective distributed collaborative production truly possible, and a new organizational form emerges: the autonomous decentralized organization (DAO).
6. From the perspective of economics, it has created a new type of algorithmic economic model. The algorithmic economy based on blockchain technology is characterized by decentralization and openness, emphasizing and respecting the voluntary principle of market transactions, and playing the role of market price. The coordination mechanism, in terms of economic freedom, has the advantages of both the planned and the market, and is an economic model closer to the free market.

Besides, we need introduce the concept of digital identity. The blockchain makes Self-sovereign Identity possible. It can itself act as a decentralized public key infrastructure (PKI) to make public key bodies more useful and secure. A blockchain can be thought of as a decentralized certificate authority that maps identity maintenance to a public key. Smart contracts can also add complex logic to implement undo and restore, reducing the burden of key management for end users. These technologies push the ownership of identity from centralized services to end-to-end services between individuals and make the identity itself controllable. This is called autonomy. This approach distracts data and calculations and pushes them to each individual, which is less economical for hackers because it requires a lot of effort to attack many personal identities one after another.

In the alliance chain, different nodes need to be assigned different permissions and meet certain supervise-ability. To this end, it is necessary to construct a secure and efficient identity authentication and rights management mechanism. An authentication mechanism based on biometrics technology or an efficient combination of biometrics and cryptography can be used. An efficient and practical identity/attribute-based cryptographic scheme can be used to achieve fine-grained access to nodes/users. Control / rights management.

Both the IBC system and the traditional PKI system are based on public key cryptography, ensuring the authenticity, confidentiality, integrity and non-repudiation of data. Security, authentication, authorization, encryption and other hardware and software facilities. . Because the IBC system takes the user's unique identity as the user's public key, the IBC system is easier to apply than PKI's huge certificate management and distribution system, and this feature is also a zero-knowledge proof framework in the blockchain system. needs.

In the public chain, it is necessary to protect sensitive information such as transaction data, address, identity, etc., and at the same time enable the accounting node to verify the legality of the transaction; for the alliance chain, when constructing the privacy protection scheme, it is necessary to consider the supervise-ability/ Authorization tracking. Trade identity and content privacy protection can be achieved by using cryptographic primitives and schemes such as efficient zero-knowledge proof, commitment, and indistinguishable evidence. You can use zksnark, mixed currency, ring signature, group signature, hierarchical certificate, homomorphic encryption, or A variety of privacy protection implementations such as secure multiparty computing.

Smart contracts have the advantages of transparency, credibility, automatic execution, and mandatory compliance. Once it is deployed on the blockchain, the code and data of the program are open and transparent, cannot be tampered with, and must be executed according to predefined logic to produce the expected results, and the execution of the contract will be recorded. It should be said that blockchain technology and its commercial applications are complementary and mutually reinforcing. Self-organizing business applications built on smart contracts can help to increase the value of blockchain technology and expand the scope and scope of the encryption economy model. Although from a technical point of view, a smart contract is just a piece of coding, it essentially carries a lot of business logic, and even a smart contract represents a business model with unlimited imagination. In turn, the realization of the self-organizing business model requires the delicate design of smart contracts, and also requires supporting technical arrangements such as performance improvement, security enhancement, and privacy protection. In other words, this is both the creation of a business model and the design of a technical system.

The security of smart contracts is still a very difficult issue, and formal verification is a worthwhile direction.

In the application of smart contracts, it is often necessary to clarify the enforceability of smart contracts from the legal level perspective where often fuzzy logic lfits for the purpose of later definition through litigation, arbitration, and other dispute resolution processes. Alternatively, smart contracts do have natural certainty and therefore do not have the flexibility and selectivity of ordinary contracts. In specific scenarios, this could prevent the establishment of an intervention mechanism that allows the code to pause or terminate execution.

# Property 4: Incentive mechanism and digital assets

Incentive mechanisms are crucial tools for inviting users to participate in blockchain governance. Leveraging non-financial incentives in public blockchains may be difficult, but not impossible in cases where historically, cryptocurrencies performed the incentive function. Permissioned DLTs are adept at aligning non-financial incentives with participants’ objectives.

## Introduce the property

Cryptocurrency is a kind of digital asset, and it includes Digital Virtual Currency (e.g. Bitcoin, AltCoins, and StableCoins) and the new experiment of Digital Fiat Currency. It is created by encryption technology, it can realize value storage, and it usually bound to a public blockchain and run on it, such as ETH on the Ethereum, the coin can be sent, received or mining.

Token is also a kind of digital asset that is issued by a blockchain-based project and can be used as a payment method for its ecosystem and gives holders the right to participate in the ecosystem network. Token represents the asset and purpose, so it can be divided into utility token and security token, which represent the specific use and company shares in the project. The token in a broad sense also has various attributes such as usage rights, income rights, voting rights, and participation rights, which can be defined as "circulant encrypted digital certificates."

Most tokens do not have the function of a digital currency, nor are they a medium of exchange. Users can purchase tokens with coins, but the reverse is not possible because tokens have specific uses or shares only in specific projects.

Based on blockchain technology, digital assets can be circulated without intermediation, which gives new meaning to token. Blockchain technology is suitable for encrypted decentralized digital certificates, but this technology is not limited to bitcoin, nor is it limited to the underlying database technology. It is also very suitable for the issuance, registration and circulation of token, and realizes value transfer. The significance of the blockchain for the liquidity of the token is shown as below:

First, the single token can be circulated at a very low cost, the same digital token can be accepted all over the world, and the digital token has no physical medium, eliminating the international Remittance costs, carrying costs, and exchange costs.

Second, the exchange cost between different token is greatly reduced. The cross-chain technology is the key to transforming the blockchain from the scattered isolated value islands into a complete value network, and becomes a bridge for the outward expansion and connection of the blockchain.

The blockchain-based Token economy can eliminate the underlying causes of the financial crisis to a considerable extent—information asymmetry, growing income disparities, and irrational sentiments, and hopefully create a new Token economic paradigm in the human information society. The distributed ledger of the blockchain turns the respective bookkeeping in the traditional business model into social public bookkeeping, and the consensus nodes participating in the data maintenance have independent and integrated data storage.

Distributed ledgers are considered to go beyond the purely technical category, and have the economic connotation of perfecting the production relationship. It is expected to realize an open organization like the Internet—DAO (Decentralized autonomous organization), which is also called “Value Internet."

The traditional Internet is an information network. The information flow is directly transmitted on the network. The value transmitted by the information flow often needs to be valued by the carrier (enterprise, bank, financial institution or third-party payment institution) that connects the value to finish the value accounting and settlement.

The blockchain is based on the design of its P2P mutual trust network, which can remove the existence of the intermediary/third party, and directly transfer the value by the consensus mechanism carried by Token/coin itself.

The blockchain-based Token economy will focus on solving the game problem of the modern economics of "game theory - mechanism design - new institutional economics - incentive compatibility", re-engagement of capital, human resources, community participation and other factors has repaired and improved the production relationship to a certain extent.

Each blockchain system can issue Tokens, and the incentive mode can be set by designing the lock period of the Token, so that the project party has an incentive mechanism to really make the project well, and because the Token of the high-quality project has an endogenous Value, which will increase social credit based on market conditions. The currency of the Token economy system is still only the legal currency issued by the central government, but the credit method is more diversified, and the relationship between the total credit value and the market situation is closer. The credit change can be more accord with the development and volatility of the economy. Since the Token of the blockchain project is anchored by the project itself, the quality of the project is the most important factor in Token's value-added, which leads to the character of Token economy system based on block chain from virtual to real. With the improvement of human informatization, the cost of exchange between different tokens will be lower, and the turnover rate of Token will be faster, and the trend from virtual to real will also be improved.

## Regulatory challenges

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

*Expressly prohibited: such as China, Vietnam, etc.*

*Strict supervision: such as the United States*

*Classification supervision: such as European countries*

*Actively support: small countries such as Malta*

With the popularity of the blockchain and its derivatives such as digital currency and Token, it will pose challenges to traditional finance and even social governance, which may have an impact on economic and financial stability. For example, with the popularity of digital assets and the increase of liquidity, the traditional monetary policy system may be invalidated, which will affect the macro-control effect. Since there is no regulated account system, digital assets are one of the instruments of corruption, money laundering, and financing terrorist activities. It is still difficult to form effective supervision. Without a third-party review, an effective principal-agent mechanism cannot be formed. Any institution that finances by issuing digital currency or tokens may cause losses to investors. At the same time, due to the borderless nature of the blockchain, a single country cannot effectively supervise it, but cross-border supervision still lacks effective practice.

Besides, there are some other new issues for regulators as below:

1. For the supervision of miners, from a technical point of view, the regulatory effect is relatively limited.
2. Regulators can selectively block through blockchain browsers, but can't do anything about illegal or false information on the chain.
3. Need to authenticate for user identity.
4. The supervision of the blockchain must follow the logic of the blockchain itself.
5. Blockchain requires laws, including blockchain security and prevention of malicious use of blockchains, and the law should also focus on the integration of on-chain and off-chain.
6. Blockchain is a trust machine, but the intervention of regulation must follow the principle that it cannot be rigid and cannot be risky, including the relationship between regulatory and governance.

## Approaches and/or recommendations

Blockchain network is a global value Internet based on cryptography theory, consensus mechanism and P2P network, and it can achieve peer to peer value transfer without third-party endorsement and settlement.

The widely used blockchain economy model is roughly divided into three types: native digital currency, public chain Token, and consortium chain Token. Native digital currency and public chain Token can be circulated in the market through trading platforms or over-the-counter(OTC) transactions, while the consortium chain Token cannot be externally circulate.

- native digital currency

The native digital currency is mostly based on the design of Bitcoin, which is considered a payable digital cryptocurrency. Its economy model has value transfer (payment), incentives for network maintainers (bookkeepers), a constant amount, and ownership belongs to a unique address.

- public chain Token

Tokens issued on smart contract platforms such as Ethereum and EOS are responsible for helping projects with early sales financing and the role of currency in the blockchain ecosystem. Its Token model is in its ecosystem: corresponding to specific rights to use/rights/benefits, incentives for network maintainers, founding teams, early investors, and ecological participants, which have a specific use in the ecology and can be consumed. A constant or deflationary economic model, with ownership belonging to a unique address.

- consortium chain Token

Tokens in the enterprise-level consortium chain often do not have an independent economic model, and are more used to carry certain rights and values ​​in the business process chain, to clarify the ownership, and to facilitate the transfer of functions.

For Token economy, there are several holders, including founding team, early investors, community operator, ecological operator and project consultants, and lock-in, redemption, and destruction mechanisms are designed to further reduce the circulation of tokens in the ecosystem to accelerate deflationary effects in the economic system, increase the value of individual tokens, and motivate Token holders to hold them for long periods of time.

The Token economy model includes incentives and penalties to reward participants in the ecosystem for the development of economic models and to penalize those who destroy the ecological balance.

 Token's circulation includes Token users, exchange platforms and wallets.

- Token users: Users can use the specific features of the project by participating in eco-rewarding tokens or using the tokens in the ecosystem. It is also possible to exchange and trade the held Token with others.

- Exchange platform: The exchange platform provides the basis for Token's circulation. The circulation of the secondary market helps Token holders to sell unused Tokens in exchange for other Tokens; or allows buyers of demand Tokens to purchase or exchange for specific Tokens.

- Wallet: The wallet serves as a Token storage tool, providing Token holders with secure Token storage and convenient transfer functions.

In addition to the network's self-generated virtual property (such as digital currency), the blockchain is more of a "mapped property" formed by offline native asset mapping, such as electronic bills, securities, equity, and other physical assets. As far as these mapping assets are concerned, the record of the blockchain is only a kind of entitlement certificate. The blockchain has the incomprehensible modification, and it cannot guarantee the authenticity and innocence of the corresponding original assets. Therefore, it is also necessary to collect data and put on chain with other technologies. In addition, the law should properly treat smart contracts. On the one hand, the law should recognize the new contract form of smart contracts, give them legal effect, and on the other hand, resolve their possible risks. The law must not only ensure the intelligent contract faithfully reflects the agreement of the parties through the inspection of the party's ability, but also respond to the irrevocable and automatic execution characteristics of the smart contract, and apply the contract change, release and invalidation system in accordance with the legal provisions.

Participants in the blockchain ecosystem include core developers, full nodes, foundations, and token holders. Blockchain governance is the process of balancing these four participants. Two perspectives of governance, one is decision-making and the other is coordination.

For DLT, the governance subject shifts from “single regulator” to “multi-stakeholder”, and the exercise of power moves from “top-down mandatory” to “bottom-up consultative”, the source of supervision shifts from “law” to “contract and soft law”. Emphasizing "on-chain governance" allows the government to participate as a third-party administrator with full access to blockchain data. At the same time, it can issue “special processing instructions” to the blockchain network. When other nodes in the network determine that the instruction is legally released, the law is invoked which also implies that a pre-configured supervisory operator can execute smart contract instruction(s).

Since the blockchain itself is a natural voting system that contains all the logic needed to change the verification assembly or update its own rules, and the voting results can be automated, the chain voting mechanism naturally becomes the blockchain ecosystem. The preferred governance mechanism. At present, there are many voting mechanisms on the chain, such as EOS, NEO, Lisk and other systems. By using the Proof of Equity (DPOS) mechanism, through the chain voting determines who operates the super-node running the network; or vote on the protocol parameters to decide the Essence's Gas cap; or to vote for a protocol upgrade, such as Teos. At present, the shortcomings of the voting mechanism on the chain are:

* Low participation in voting, which leads to two problems.
	+ The results from voting may only reflect a small number of peoples’ opinions making it difficult to get universal acceptance of voting outcome;
	+ The attacker can cast numerous votes with a small amount of cost. In such a case, there may be a fiscally strong minority in control of governance that harms the interests of ordinary users. At present, relevant events have occurred.

Therefore, in addition to the on-chain voting mechanism, it is necessary to explore other appropriate on-chain governance mechanisms.

In addition, relying solely on-chain governance, it is still unable to solve the principal-agent problem of the blockchain ecosystem, and it also needs legal intervention, chain governance and supervision support. How to improve the governance mechanism on the chain is the research direction of the next DLT technology.

# Property 5: Openness and transparency

## Openness and transparency *also imply that data’s integrity (accuracy), confidentiality (privacy) and privacy (usage) can be simultaneously protected.*

Several key properties featured in Distributed Ledger Technology (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 from governments and companies alike.

The debate regarding the level of openness and transparency from DLTs should start at the discussion on *Permissioned* and *Permissionles*s Ledgers, where *permission* refers to how the system works with respect to validating transactions. On permissioned systems, you need to be approved beforehand in order to put yourself as a validator node in the distributed network. This implies that peers know each other, to *some* extent.

A permissioned DLT is normally deployed by private organizations or individuals in a particular way, by which it is not anyone that can perform *read/write/validate/audit* operations on any given transaction. Usually, the *write* and *audit* permissions are kept centralized, while the *read* permission may be public (or restricted to the limited group of people). In permissioned DLTs all the decision-making processes derive from a trusted third party that has exclusive roles among the network players, especially granting them access to its content and assigning the aforementioned permissions to each new player. They are, in general, more optimized if compared to massive open DLTs when it comes to speed, scalability and data privacy. In this regard, everything is also secured by strong tools from applied cryptography, however, this does not fully eliminate challenges and trust issues.

On the other hand, as the Bitcoin and Ethereum networks show, on permissionless Blockchains all the peers can act freely, entering or leaving the network at any given time, without identifying or authenticating themselves in a formal sense and without causing any disruption, recognizing these systems offer no confidentiality at all. Everything can be set in a pseudonymous way solely by running code. They allow every user to create a personal address (actually, an infinite amount of them) and to begin interacting with the network by submitting transactions and broadcasting their own entries to the distributed ledger. Public DLTs are based on different consensus algorithms which are mostly open source and everyone can perform read/write/audit actions regarding transactions in the network, with no need for a trusted third party. Moreover, any party has the choice to establish a verification or even a validator node (also known as a “mining” node in the Blockchain jargon) to actively help transactions to be confirmed and unequivocally accepted by everyone else.

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 its 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 to a certain degree established by a central party.

*Openness/Transparency*

Broadly speaking, transparency is generally associated with openness and visibility, or the opposite of secrecy. Considered a necessary element for the development of democratic systems and civil participation, transparency is believed to empower the weak, while holding the powerful accountable – therefore reducing the asymmetries between them (specially concerning information availability).

Notwithstanding, this “narrow” view of transparency fails to address some nuanced relations, as for normative dimensions. Those complex relations or systems require more clear answers to some questions such as: what is to be disclosed? to whom? when? for how long? how (in terms of the quality and accessibility of information)?

Confronted with those issues and aware that unchecked transparency could also generate negative externalities (such as hinder individual privacy, enable more surveillance and control, create an overload of information leading to disinformation) some believe that transparency is “losing its innocence” (Arthur P.J. Mol, 2013).

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.”

To this more inclusive definition we should also consider that it does not yet answer fully our question to the limits of transparency. Again, conscious of the negative externalities that could be generated by the full extent of transparency, different systems will have to design their appropriate level of transparency regarding what should be disclosed and to whom.

In relation to DLT technologies, originally the core idea behind them was that their platforms would not have a central authority to control it. For that to happen it would have to be a completely open platform, allowing anyone to transact or even to run a node. But also, a transparent network, by allowing anyone with access to the network to read the history of all the past and present transactions in real time.

Public DLTs record work through common shared databases, to which all parties can propose changes. The network automatically validates new information, while anyone connected to it could audit the entire process, guaranteeing the rejection of wrong data and the confirmation of proper information, periodically re-establishing the public consensus. Here the decision-making process is normally done by either one or a mix of possible consensus algorithms that secures decentralization, mostly Proof of Work (PoW) or Proof of Stake (PoS). It thus allows everyone to see the all the data, as each and every peer has the exact same copy of the database, with verified new information being added to it. This public audit capability makes for the system indisputable groundbreaking level of transparency.

Since the beginning the openness and the transparency features of DLT platforms were praised for the contributions it could provide, not only in the economic sector, but also in the social sphere. Form the social perspective, transparency would be paramount to empower every participant in the network, leveling everyone by offering access to information. That element is the cornerstone of the idea of the DLT as a trustless system, since for being open and transparent it would deal with corruption and malpractice by possible spoilers. Transparency is also essential for collaborative decision making, generating incentives for interactive effects among independent participants.

From the economic perspective, transparency in DLT systems would unlock the potential of new economic models based on the complete access to information. It has the potential to impact positively the sharing-economy business models, as an alternative to the traditional exchange economy. These collaborative models have been used at the local level or even a bit wider, when powered by the internet, whereas DLTs make it possible for them to operate globally if needed. Albeit Permissioned DLTs are not necessarily required to be open and transparent, they usually chose to have a reasonable level of openness and transparency (depending of the business model of the central player) so they could also benefit from the advantages.

From the perspective of self-agency, a sole actor may wish to memorialize information about an autonomous transaction in sequence. Furthermore, committing information to a publicly accessible DLT protected by encapsulation a Digital Object might be deemed necessary.

The Edge is where our digital information is found. The Edge is where the Internet finds us. Often in the past, we relied on centralized or federated entities to protect the confidentiality, integrity, and access to digital information. As new technologies shift processing resources nearer to data sources, a way to augment protections in a decentralized manner may render some external dependencies unnecessary. For instance, Autonomous Transactions, might be logged in sequence to a DLT with only labels or headers viewable in plaintext. Such data-aware labeling informs only an authorized Relying Party precisely how to discern trustworthiness and unlock data based on certain privileged awareness.

Publicly accessible registries can be used by anyone with knowledge about access control mechanisms to: a.) Determine when to initiate or join information cohorts; b.) Post information and enable others to resolve queries to discern ‘safe-to-proceed’ signals. (e.g. when authorization, control intention, and settlement/finality acknowledgment messages have been logged to initiate and complete an atomic transaction).

When used as a source of truth about sequence and data fidelity, DLTs might achieve outcomes faster, with less risk, and with superior accuracy with less complexity than other Application Control Architectures.

## Regulatory challenges

Even though Openness and Transparency are often regarded as major positive features from DLTs, enabling them to be more trustworthy and secure also pose some challenges in certain circumstances. Distributed ledger platforms generally work on an allegedly “paradox”, in which, while the information on the ledger is transparent for everyone to see/read they are also private, 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 to confer to the individual the control of their own personal data, therefore not allowing it to me fully transparent and open to everyone. In 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 fiscal evasion, money laundering and funding criminal activities.

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

## Approaches and/or recommendations

Openness and Transparency are often two of the major features to deal with ‘trust deficits’ from any application/solution. Once implemented, the processes become more accountable by allowing every participant to see/monitor the transactions and procedures through DLTs, since they were first conceived and are intimately related to those two features.

Notwithstanding, despite the general agreement on the positive impact that openness and transparency often offers, as seen before, they might also pose some challenges for certain sectors. In this sense, it is recommendable that each DLT protocol and governance adjusts its level of openness and transparency according to two major factors:

* Regulation. Currently many countries are currently reorganizing or developing their legislations to create codes to govern issues such as privacy, data management and other themes related to the internet, but also new applications as cryptocurrencies. DLTs platforms such take in account those regulations to be able to comply with their directives.
* Sector. Each sector has each particularity. The financial sector has different demands and requirements if compared with the education or the health sector. An efficient solution requires an appropriate DLT platform and a well design application.

On the flip side, regulations will also have to evolve. DLTs, as any emerging technology, are often subjected to a certain degree of distrust and doubt. Especially because, often, some of the early users take advantage loopholes in the unregulated scenario to engage in questionable or illegal activities. That dynamic tends to weaken the position of emerging technologies toward legislators.

To deal with this issue, it is highly recommended to foster an informative and high-quality political dialogue with public authorities and legislators, in order to encourage enabling legislations rather than only prohibitive ones. Prohibitive regulations would create disincentives to innovation, which could significantly hinder the preferred outcomes from emerging technology.

# Property 6: Anonymity

## Introduce the property

Transactions on DLT can be used to hide the identity of actors. The identity can be hidden from everyone that is not part of a transaction and even from the partner of the transaction. Many DLT systems do not require identification at all and a few do provide strong anonymity – the implication is that breaking anonymity with conditional access controls to ensure identification is generally not possible.

However, despite the fact that Bitcoin neither requires identification nor provides strong anonymity, there are services available that can identify the entity that is behind a bitcoin transaction. These services are used by law enforcement and tax authorities.

## Technologies for strong anonymity

The ISO/IEC 20008 standard specifies 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.

In their 1991 Group Signatures paper, Chaum and Van Heyst presented "a new type of signature for a group of persons" [ax]. The group has "numerous members and a single manager", all associated with "a single signature-veriﬁcation key", the "group public key" [bx]. Each group member has "its own secret signing key" with which a member can produce digital signatures that can be verified using the group public key [bx]. Signatures created by different group members are "indistinguishable to their veriﬁers, but not to the group manager" who can disclose the identity of any group member [dd].

As described in their paper [ax], the group manager has a secret master key with which it can "extract the identity of the group member who created" a signature from a given signature instance [bx]. This capability provides the property of signer traceability. Given a group signature, no one without possession of the secret master key held by the group manager should be able to determine which group member was the signer. This capability provides the property of signer anonymity, where the larger the group size the more anonymity is provided.

Group signatures are anonymous digital signature mechanisms in which a relying party uses "a group public key to verify a digital signature" of a group member [op]. Some group signature mechanisms may be capable of revealing to any verifier information about the signer, such as the capability to link "two signatures signed by the same signer" or the capability of a "special entity to reveal the identity of the signer" by opening a signature [op]. Some group signature mechanisms have both a linking and an opening capability.

Some group signature mechanisms provide additional properties such as revocation. Three levels of revocation may be performed by a group manager of group signature mechanisms. The entire group may be revoked, a single group member may be revoked, or specific signing capabilities of one member may be revoked. Up to four possible revocation types are described for the group signature mechanisms defined in the ISO/IEC 20008-2 standard. The available types vary by mechanism and include private key revocation, verifier blacklist, signature revocation and credential update.

In contrast to group signatures, ring signature schemes do not support revocation of any type. They do not have group managers, require "prearranged groups of users", or management "procedures for setting, changing, or deleting groups" [dd]. Since there is no group manager, it should be possible to determine the identity of the ring signer only from self-disclosure. There is no group setup procedure, so ring signatures schemes only require a signer private key and the public keys of an arbitrary set of all of the possible signers to form a ring.

All a signer needs to do to create a ring signature is to choose the ring members. No permission is required to use the public keys of the other ring members or to include them in the ring. The signer needs no assistance or cooperation from the other ring members to create a ring signature, just access to their public keys. Since the signer is included as a member of the ring along with the other non-signer members, the signer must send the signed message through an anonymizer to mask its origin.

## Regulatory challenges

Between anti-money-laundering statutes and KYC requirements on the one hand and data protection laws on the other hand there is not much leeway. Blockchains that neither provide identification nor anonymity might actually be in violation with both.

AML and KYC laws require identification towards the other party of a transaction, towards intermediaries that are in charge of checking compliance and towards law enforcement. Data protection laws require that identities are not disclosed to anybody else. They also require that identification will not be available anymore after the legal requirements have expired.

Using cryptography to design privacy by design has a specific challenge in this situation. While an intermediary that controls the access to information stored in a database has no technical restraints in providing access to information in deciding when to delete some information, rules coded in cryptography cannot be changed afterwards. This provides superior protection to privacy but it is a challenge whenever compliance requirements change or require a differentiation of disclosure that is hard to code into a cryptographic system.

## Approaches and/or recommendations

Examples of approaches and/or recommendations for users, regulators and solution providers to address the challenges associated with this property

State-of-play and future considerations pertaining to Zero Knowledge Proofs:

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

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

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

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

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

Challenges to the wide application of ZKPs have been:

1. They can be slow and expensive for proofers to process. This has now been addressed by the October, 2018 release named, “Sapling.”
	* Viewing keys allow owners of shielded addresses the ability to view transaction details without exposing their private spending key. Additionally, these can be shared with trusted third parties for compliance, auditing or for other reasons. Previously, only incoming transactions were viewable.
	* Efficiency improvements in Sapling’s key signature processing extends the capability of the viewing key to include visibility into outgoing transactions for a shielded address. Visibility can include the transaction value, memo field and target address.
2. Some identity solutions use ZKPs based on graph isomorphisms, and these are exceedingly fast in comparison with other ZKP variants; and
3. Questions remain on the interoperability of ZKP-based credential exchanges.
	* As the aforementioned Sapling example suggests, guiding principles for a Gateway Protocol might include: “Be liberal in what you receive / Be conservative in what (and how) you send.”
	* While there are many ZKP variants, with a wide range of performance characteristics, they are still to be considered in early stages of development;

Presently, standards for a universal applicability of zero knowledge proofs across implementations and technology suppliers do not exist.

To further complicate matters, as IoT and other sources of data emerge, there is the need to protect business processes that release real-time transfer instructions that can only execute upon verification that the following conditions apply:

1. The digitalized attributes of an intended receiver of an information transfer are accurate
2. Time-sensitive duties are legally enforceable; and
3. Bi-lateral information flows are protected by strong access and usage restrictions for the following outcomes beneficial to Relying Parties:
	1. Anonymity
	2. Autonomy
	3. Atomicity

## References

[ax] Chaum, D., & Van Heyst, E. (1991, April). Group signatures. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 257-265). Springer, Berlin, Heidelberg. Retrieved September 2, 2018, from https://link.springer.com/content/pdf/10.1007/3-540-46416-6\_22.pdf

[bx] Bellare, M., Micciancio, D., & Warinschi, B. (2003, May). Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 614-629). Springer, Berlin, Heidelberg. Retrieved September 6, 2018, from https://link.springer.com/content/pdf/10.1007/3-540-39200-9\_38.pdf

# Property 7: Autonomy

Autonomous definition as having the right or power of self-government, relating to or marked by autonomy is an essential consequence of a capable of existing independently.

## Introduce the property

Transactions on DLTs can be executed autonomously. This implies that a self-governing organization, network or institution can be driven via autonomous agreements or Smart Contracts. Smart contracts can automate most of the smaller processes typically associated with a legally binding contract. Ultimately, smart contracts give people and organizations a level of autonomy, security, privacy, speed and ease of use, cost-savings, immutability, accuracy, reliability, and trust that no centralized third-party can match by just adjusting their rules of administration by Smart Contracts.

Therefore, Autonomous property in this section is going to be considered as a binomial component:

1. Smart Contracts (SC)
2. Governance-less or self-governing

Functionality of the Smart Contract is under continuous ongoing with development and code deployment everyday which is an indicative of the reality and useful argument for a new environment of performance. Thru SC can be possible to modulate the governance and automate the human behavior on a networking/organization/entity within DLTs system. Any voting process can set the rules by SC and being trace uniquely.

The enormous applications of SC allow infinite formulas to adopt rules and performing transactions which are recorded on a Blockchain or DLTs. A competent component which is upgraded and developed by the users is a perfect ingredient for decentralized autonomous organizations and this fact is an evidence with the proliferation of DAOs and autonomous models of governing people, entities, things and processes. And further sophisticated assembly models like Decentralized Altruistic Communities in a new exercise of freedom of association based on Blockchain and DLT frameworks.

With the rise of awareness for data privacy, end-users have become reluctant to share their data. Also, in another perspective, user data are becoming a valuable asset. Therefore, it is meaningful to develop a reliable infrastructure in which end-users or data creators are able to securely transfer data in a privacy preserving manner and get compensated for their contributions by a cooperative deep learning task on a blockchain empowered cooperative deep learning mechanism ( see at… <https://arxiv.org/pdf/1807.02515.pdf>).

Challenges associated with this property

Heterogeneity: state consisting of diverse components (added by a natural way of work).

Interoperability: it is necessary to deploy policies by the DLTs frameworks whereby check or access points or gateway allow the users to connect their DLT systems with others DLTs system of Blockchain ecosystems in a secure way as their will.

Conflict of interest and discoverability: how the interest could be autonomously resolve is a critical part however an interest could be further than just an interest and decentralized applications can interact between them and new discoverabilities may faulted a dispute.

Maintenance: a neutral or balance maintenance it is another challenge associated with the property in particularly is a clear state of the art based on test-net before launching a public usable version at a main-net for instance.

## Regulatory challenges

Civil liability as a potential responsibility for payment of damages or other court-enforcement in a lawsuit, as distinguished from criminal liability.

Criminal liability as a potential responsibility of punishment for a crime.

Smart Contracts are built by programming languages which allow to be incorporated as component of an autonomous DLT system, such coding procedures some times are open source licenses and users are not dully aware about the disclaimers or simply it is bad habit to avoid it or miss the disclaimers and alerts just by usable and suitable interoperability, this within open source software although have their normative and regulatory space on blockchain and DLTs systems can be a combination that is not easy to determine. Smart Contracts is one of the key elements to maintain a self-governing or an autonomous model, however is in continuous deployment by developing the code adjustments and the dynamic life of the framework, so it is not static exercise for the regulatory bodies, neither easy to implement by local administrative adoptive rules prior to the regulatory ones, which it does not happen by SC modeling onto some decentralized and autonomous organizations.

The IoT and blockchain shall disrupt areas whereby the IoT can predetermine effect autonomously and this with AI will bring a new paradigm of post-humanity between trans-humanity whereby the regulatory challenges are not only socio-economically considered.

Protection of third parties is another challenge which is associated with the former mentioned above, however an autonomous mechanism of governing and performing can incur immature with a rigid consensus based in regulatory aspects and laws by the stakeholders or the off-chain ownership. In this futurist century we are disrupting as human beings all the areas we have discovered thanks to the technology and the regulation, it is an essential part of the relationship between both for the sustainable and developments goals.

**Automatic decision-making**

Insert discussion here. GDPR has guidance on Natural Persons as ‘whoever has the key to an account and signs for access has control.’

Permissioned blockchain, then there is control according to the origin agreement. Other use cases where a solution is offered but packs everything together by using the blockchain – inside the application things are transparent to the blockchain with not real control over it, but the application takes over the control. Have to see different scenarios. When you have control, over blockchain, it increases your responsibility. Introducing all control features, then compliance requirements rise as well. Deleting data in the context of GDPR is not an exception but the rule, if you apply this in every case, you void the trust in the blockchain.

Certain time-to-live requirements, blocks older than ten years must be erased…when fraud has been committed more than ten years ago, it will be impossible to prove a fraud has been

**Regulatory issue for further study:**

A condition might arise with a smart contract where intervention during the entirety of the data lifecycle is impossible. In such a case, dispute resolutions may be resolved by logs proving that the keys used were in control of a duly authorized and responsible entity.

Absent such auditable evidence, a problematic ‘in-between’ condition arises: reliance on a smart contract that one cannot control that operates on a permissioned blockchain that one does control. Such in-between cases should be avoided. The people with control over the permissioned blockchain with full autonomy would have duties to perform functions of a fully autonomous private smart contract. This is a dire warning to people who say, “Just use permissioned blockchains and you are okay.” Nope, you are not. Understanding such nuance is important.

## Approaches and/or recommendations

With regards to Open Source and Free ‘Libre’ software licenses, there are some interesting efforts by Open Source Initiative and other organizations. Open-sources license comparisons can found at this link: <https://en.wikipedia.org/wiki/Comparison_of_free_and_open-source_software_licenses>

Further to specifications like the European Union Public License (EUPL and their compatible free software) there is a key component as a recommendation in this challenge which is the copyleft as a general method for making program free and represent an incentive for other programmers to add to free software and Copyleft is based legally on copyright, so the work should have a copyright notice as a copyleft type license. However there are others scenarios whereby the copyleft does not exist and the only recommendations are based on the readiness and understanding of the license per se which sometimes are variables from others and there is a common practice to recommend disclaimers like *“this is an open source software please note that the distribution is your responsibility with your customers”*, therefore the recommendations are based on the end-user information how is informed updated and upgraded and alert about this aspect by a repetitive disclaimer regularly by periods. These parameters are also useful to determine the civil liability and try to reach insurance within the areas that are not covered in nature by the infrastructure or the DLT system.

Protection of third parties can recommend policies of an alternative dispute resolution prior to an off-chain solution. It is recommended case by case however there are associative initiative within the scope of International Consumer Protection and some Acts and law that are suitable as a recommended compartments when policies are described for a DLT system.

For the IoT there are some rules like 5G laws in different jurisdictions but is also recommended the new ISO/IEC 30141:2018.

Examples of approaches and/or recommendations for users, regulators and solution providers to address the challenges associated with this property.

# Summary

Table n: DLT features and regulation challenges

| DLT features | Regulation challenges | Conformance, recommendations (for users) | Regulatory recommendations (for regulators) | Technical solutions (for vendors) |
| --- | --- | --- | --- | --- |
| Distributed fashion | 1) territorially of applicable law multiple nodes established in multiple jurisdictions;2) who will be legal subject;3) distributed storage solution need developed to meet the requirements of the prod environment4) Interoperability requirements |  |  | IPFS, sia and other distributed storage projectOff and on chain enforceability |
| Tamper evident and tamper resistant  | 1) immutable shared ledgers, error corrections mechanisms2) right to be forgotten3) smart contracts4) … |  |  |  |
| Shared ledger | Privacy & data protectionIn a DLT network, data, including certain customer information and transaction records, may be shared by all parties on the network. Even where such data is encrypted, it may be vulnerable to being exposed or accessed by undesired parties on the network [FINRA, «Distributed Ledger Technology: Implications of Blockchain for the Securities Industry» , 16]How to protect user data (password…) in open environment?How to mitigate risk of data abuse in open environment?The security issue of blockchain system, include smart contract, not only on-chain data protection.… |  |  |  |
| Incentive mechanism and digital assets  | 1) what is token/coin?2) what kind of ICO is legal?3) what’s the next crypto-economy system, not only the current token economy?4) …A DLT network designed to facilitate securities transactions may present new and unique challenges related to maintaining appropriate supervisory policies and procedures and surveillance systems in accordance with applicable rules (*see, e.g.,* FINRA Rules 3110 and 3120). For example, FINRA’s supervisory rules require the review of customer account activity as well as the review of post-trade transactions, such as account designation changes, to correct order errors… [FINRA, «Distributed Ledger Technology: Implications of Blockchain for the Securities Industry» , 18] |  |  |  |
| OpennessTransparency | Abuse, e.g., financial crime, abuse images, dark web links, wikileaks… |  |  |  |
| Anonymity  | 1) noname users vs identification (AML/KYC) |  |  |  |
| Autonomous  | You cannot stop SC executionYou can automatize your rules for governing  | <https://eupl.eu/> | <https://www.iso.org/standard/65695.html> | 1.Checkpoints2. Open Access  |

Appendix I: Security issues in DLT
(asymmetric Public Key cryptography issues)

The use of DLT-systems in Russia requires first resolving the following issues related to trust frameworks that utilize Public Key cryptography for authentication:

1. For each node of DLT-system the following should be provided:
2. the possibility of trusted installation of root certificates used in the system of the certifying center (certification authority);
3. Each node of the DLT-system must have real-time availability of up-to-date information on the status of certificates of the remaining nodes of the DLT-system. (for on-demand checking of the electronic signature);
4. It is required to determine the need for an interface to work with a Certification Authority (CA) to obtain information on the status of certificates (CRL or OCSP),
5. Either as a separate interface (within the described node interface for interacting with non-DLT systems) or
6. Within the administration system (adding to the possible duties of the administrator of the DLT-system in the receipt / distribution of CRL).

In terms of key management, it is necessary to indicate the existence of a limitation on the validity of the private / public keys of users / nodes, as well as recognize the conditions of possible key compromise. Furthermore, technical issues such as:

1. Key changes
2. Revocation of certificates,
3. Potential severity of harms caused by an inability to use the public key after it expires to perform the electronic signature verification of blocks, rendering data in "old" blocks of distributed ledger unavailable.

These technical issues concerning the validity of keys are highlighted in these circumstances:

* When there is the need to change the node ID when it is calculated from the public key (as was done in Ethereum and Masterchain)[[1]](#footnote-1)
* When there is the need to check the correctness of the electronic signature not immediately, but at the time of signing the block / transaction … for these tasks, one can use the formats of the “improved” signature - some CADeS or other variants - and the procedures accompanying them.

DLT-based tools such as Smart Contract might respond in any number of ways when encountering an expired digital certificate. For instance, in DLT contexts, a certificate may be used to digitally sign a field, a transaction, or on a block of transactions. An expired certificate can occur anywhere in the validation path, from the end-entity certificate holding the signature verification key, all the way up to a trusted root certificate.

Examples of behavior we discussed included widely used internet applications for email and browsing (e.g., Outlook, Internet Explorer (IE), etc.). Perhaps due to their internet context, such applications react to expired certificates by interrupting processing to alert users of potential signer identity trust issues. Users are detained, prompted to read an alert, then allowed to cancel or continue with their activities.

In this internet context an expired certificate is treated as an unexpected and potentially harmful event. Internet application behaviors seem focused on protecting users from expired certificates, almost to the point of treating them as children about to run into a busy street. For the DLT context, a different model of application behavior is needed. This new model should expect the occurrence of expired certificates due to the long lived nature of a ledger. Except for when used to sign data, encounters with expired certificates should be treated as a normal course of processing blocks of data in DLT.

ITU-T Recommendation X.509 section 12 "Certification path processing procedure" is used by a relying party to determine whether a particular certificate is trustworthy. In section 12.5.1 the basic public-key certificate checks include determining that the signature verifies, the certificate dates are valid, and that the certificate has not been revoked. In a DLT context a relying party has this same goal at the point in time that data is being signed.

At a later point in time, a DLT relying party has a somewhat different goal. They seek evidence that a past signature event can still be trusted. They wish to know whether a public-key certificate associated with a signing key was trustworthy when an object was signed, even if associated certificate dates are no longer valid. Both of these cases are supported by X.509, but support for the latter case is not readily apparent in some internet applications.

In a DLT context, a timestamp in the block header indicates the time the block data was signed. It is arguable that signed, timestamped DLT objects differ from typical signed internet objects in this way. DLT can be treated as a new application of PKI, one that differs from its use in internet mail and browser applications. There is an opportunity for useful ITU-T standardization that recognizes these differences between an internet and DLT contexts and that normalizes the expected behavior of PKI-based DLT applications.

There are two areas of standardization needed to support interoperability and growth in PKI using DLT applications. 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 results in tool behaviors that do not obstruct ledger processing.

A profile for X.509 certificates used in a DLT context should be standardized by ITU-T. This would serve a similar purpose as the IETF PKIX profile for internet certificates. A DLT profile could recognize the full sweep and global nature of DLT. 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 DirectoryString, replacing the common, historic use of PrintableString (US ASCII) types.

An X.509 certificate profile could normalize the use of GeneralizedTime over UTCTime to ensure that DLT supports dates beyond 2049. Use of GeneralizedTime would simplify the implementation of ledger searching that typically involves mixed two-digit and four-digit year data. Normalized time and date data could enhance the chances of achieving interoperable DLT applications and support cross-ledger data flows.

A DLT certificate profile could normalize a set of certificate extensions supported by all DLT applications. DLT applications can benefit from assurance that certificate blacklist information is readily available at the time of signing and at the time of subsequent verification. A consistent, common approach to providing blacklist data would allow tools developers to more easily support third party access to DLT systems and enable audit and assessment functions.

A profile normalizing the inclusion of the cRLDistributionPoint extension in certificates supporting DLT applications is one example.  This extension could ensure that blacklisting was available by default for all signature verification. Other certificate extensions and their handling could be profiled to advantage as well.

Section 7.13 "Repudiation of a digital signing" of X.509 already provides the basis to support "the revalidation of the digital signatures of data" for DLT signatures after certificates have expired. Section 7.13 allows DLT timestamped information to be included as an input to certification path validation processing. This could serve as the starting point for normalizing DLT-specific revalidation processing that relies on the input of the "certificates, CRLs, and timestamps that were used in the initial validation process".

The normalization of DLT-specific path validation processing could lead to a common set of tools behaviors and industry best practices. Such standardization would serve as core DLT technology. PKI processing would be vendor neutral and could be commonly adopted to establish norms at a level that did not interfere with vendor competition and innovation. Instead, such norms could lead to greater public trust in DLT solutions.

Appendix II

Blockchain/DLT is just a tool that is being used by different parties for both good and evil.

If we talk about blockchain as an instrument to combat old types of corruption, we must also mention that it can be (actually, is) used as a basis for new types of corruption which is much more difficult to prevent.

The same can be said about transparency. Blockchain/DLT solutions can be used for combatting unwanted transparency; and smart contracts even more so.

Blockchain is widely considered as a potentially useful tool for combatting corruption and ensuring transparency. Most potential use cases are related to the degradation of trust into public institution in certain countries; and frankly I don’t believe that purely technical measures will be truly helpful. If you’ve got a failed state, you should rebuild it first.

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

There are so far less widely spread concerns that Blockchain/DLT could be also used to avoid transparency and support innovative types of corruption. Anti-corruption, pro-transparency measures should be considered early at the design stage, taking into account intended application of the solution. Unfortunately, at present the focus is mostly on privacy (including transaction privacy) protection which is, of course, also quite beneficial for corruption-supporting applications of blockchain.

Lack of designated owner / responsible person in public permissionless blockchains, combined with trans-jurisdictional operations, also hinder public oversight and law enforcement. To whom will you send the subpoena?

Properly designed smart contracts may eliminate some root courses of corruption by ensuring fair access to goods and services without interacting with potentially corrupt humans. But they also could be used for smart collecting of bribes. That means that in many application areas some vetting system for smart contracts and means to remove them are needed.

**Bibliography**

[b-NIST]

1. [Conceptualising DLT Systems : University of Cambridge (Judge School](http://www.paymentpathways.com/wp-content/uploads/2018/11/2018-08-conceptualising-dlt-systems.pdf))
2. [Alastria presentation Rio January 2019](http://www.paymentpathways.com/wp-content/uploads/2019/01/2019JAN15-Alastria-ITU-Presentation-Rio-de-Janiero.pptx%20%20%20%20%20%20%20Richard%20O%E2%80%99Brien%2C%20VP%20Financial%20Services%20InterComputer%20Corporation%20200%20S.%20Wacker%20Drive%2C%2031st.%20Fl.%20Chicago%2C%20IL%2060606%20312-346-9400%20%28w%29%20312-270-3680%20%28m%29%20%20%20Rick_O%E2%80%99Brien%20%28WeChat%29%20richard_obrien%20%28Skype%29).
3. [OECD Antitrust details](https://one.oecd.org/document/DAF/COMP/WD%282018%2947/en/pdf).
4. [Anti-trust article](https://mcdonaldhopkins.com/wapi/Pdf/View?url=https://mcdonaldhopkins.com/Insights/Blog/Business-Insights/2018/09/19/Blockchain-technology-Antitrust-risks-and-safeguards)
5. Blocks as Digital Entities: A standards perspective, P.A. Lyons & R.E. Kahn [add cite]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. DECENTRALIZED NETWORK FOR DATA EXCHANGE AND STORAGE "MASTERCHAIN" //Version 1.1 // WHITEPAPER Association for Financial Technologies Development Moscow, 2017// <http://fintechru.org/documents/Masterchain_whitepaper_v1.1_en.pdf>. [↑](#footnote-ref-1)