TECHNICAL SPECIFICATION

ISO/TS 23635

First edition
2022-02

Blockchain and distributed ledger technologies — Guidelines for governance

Reference number
ISO/TS 23635:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document addresses how key governance characteristics such as decision rights, accountabilities, and incentives operate effectively and efficiently in DLT systems.

Due to the fast-evolving nature of DLT systems and their adoption, this document has been developed at a level of abstraction to provide guidance and instruction in diverse contexts. “Distributed ledger technologies” (DLT) includes blockchain technologies. The specific blockchain technology will be named explicitly only where specific characteristics of blockchain technologies warrant doing so.

DLT systems challenge our existing understanding of governance as these systems are often decentralized in their governance. In the case of permissionless public distributed ledgers, they can comprise an unrestricted number of potentially pseudonymous DLT users and nodes. Even permissioned public blockchains can have hybrid governance structures, comprising elements of centralized as well as decentralized governance. In the absence of a central governing authority for distributed ledger systems, several governance questions regarding ownership, decision rights, responsibilities and accountabilities, and incentive structures emerge that cannot be addressed by applying traditional governance mechanisms.

Thus, for distributed ledger systems, it is important for participants to establish who they are dealing with (identity) and who is responsible and accountable for the directing and control of the DLT system (governance). For organizations and broader industries, it is difficult to engage in the development of DLT systems in the absence of effective DLT-governance mechanisms.

In general, DLT systems aim for decentralizing decision rights and the technical implementation of accountability. The locus of achieving consensus is decentralized, meaning that the records that form the foundation of the DLT systems are not only distributed but also in many instances validated by multiple DLT users. Moreover, disagreements can be resolved in a decentralized way if users initiate ‘forks’ by copying and branching existing codebases and developing them further according to differing goals.

As DLT systems gain importance, incentive alignment becomes increasingly important. While incentives are at the core of all economic activities, in DLT systems aligning incentives adequately is important for effective functioning because in many DLT systems incentives provide the means of achieving consensus. Unless incentives are properly aligned, the nodes of the DLT system will not contribute to consensus. Improper incentive alignment threatens the integrity of the system and can prevent a DLT system’s effective functioning.

Smart contracts can allow for decentralized governance mechanisms, but many present-day DLT systems continue to be characterized by a degree of centralized, often informal, decision-making. In DLT systems, accountability in principle will increasingly be implemented technically rather than institutionally through traditional contracts.

Smart contracts allow for specifying and enforcing accountability using codified rules on-ledger. However, in some cases it is not possible to implement autonomous transaction enforcement completely on-ledger. In these cases, some form of off-ledger institutional involvement can be necessary for effective dispute resolution among DLT users. The establishment of ‘off-ledger’ governance instruments will be beneficial in assuring participants in the integrity of DLT systems.

Standards in these areas will also benefit DLT developers and providers looking to establish new DLT systems that provide confidence to stakeholders. A key accountability issue concerns identity in DLT systems, usually granted through the public addresses that are used to conduct transactions in public DLT systems. Given multiple and pseudonymous identities, this could be a problem. Some users will wish to identify themselves using traditional institutional means (e.g. driver licenses linked to their DLT identities). Other technical approaches can seek to address the problem of ensuring confidence in user identity, for example by linking reputation to public addresses. Overall, the shift toward the enforcement of accountability through technology has only begun and it is likely that institutions will continue to play important roles for ensuring accountability in DLT systems for some time to come.

This document is organized as follows. Clause 4 presents governance principles for DLT systems. Clause 5 discusses the governance framework for DLT systems. Clause 6 discusses the governance of different types of DLT systems. Clause 7 the lifecycle of DLT systems. Clause 8 discusses the roles involved in the governance of DLT systems. Clause 9 discusses governance instruments for DLT systems. Clause 10 examines governance considerations of the interoperability of DLT systems.

The audience includes but is not limited to academics, architects, participants, users, developers, regulators, auditors, and standards development organizations.

Blockchain and distributed ledger technologies — Guidelines for governance

1 Scope

This document provides guiding principles and a framework for the governance of DLT systems.

The document also provides guidance on the fulfilment of governance, including risk and regulatory contexts, that supports the effective, efficient, and acceptable use of DLT systems.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22739, *Blockchain and distributed ledger technologies — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
distributed ledger technology governance
DLT governance
system for directing and controlling DLT systems including the distribution of on-ledger and off-ledger decision rights, incentives, responsibilities, and accountabilities

3.2
governing body
entity that is accountable for the performance and conformance of the distributed ledger technology governance

4 Governance principles for DLT systems

4.1 Overview

This clause sets out nine action-oriented principles for good governance of DLT systems that will be elaborated in more detail throughout the document. The principles are intended to help stakeholders evaluate and improve governance mechanisms, structures and activities, with a view to meet governance objectives, which are: effective, efficient, and acceptable use of DLT systems. This is primarily achieved by providing stakeholders with the right incentives to perform their roles within a governance framework.

The governance of DLT systems should include commitments to address sustainability issues in their establishment, operation, and termination.

NOTE Useful sources of information on sustainability issues are ISO 26000 and UN Sustainable Development Goals (SDGs)[15].

The governance principles provide the foundation for implementing mechanisms, structures, and activities in DLT systems. The statement of each principle refers to why it is important and what should happen, but does not prescribe how, when or by whom the actions must be implemented, as these aspects are dependent on the nature of the DLT systems.

4.2 Principles

4.2.1 Principle 1: Define identifiers of entities involved

DLT systems can vary in terms of the identifiers of the actors of the systems. Some DLT systems use pseudonyms as on-ledger identifiers while others use off-ledger identifiers to provide confidence. The definition of identifiers appropriate for the DLT system is the foundation for all governance functions.

4.2.2 Principle 2: Enable decentralized decision-making

Decentralization of decision-making is a key characteristic of many DLT systems. Decision-making in DLT systems can either be embedded on-ledger or off-ledger. Decentralized systems foster participation in collective decision-making, thereby enhancing overall trust. DLT systems should enable decentralized, on-ledger decision-making processes. When decisions are made off-ledger, they should be made in an explicit and formal manner.

4.2.3 Principle 3: Ensure explicit accountability

Over the lifecycle of DLT systems, ownership and decision-making rights can change and thus, so does accountability. Due to the decentralized nature of most DLT systems, explicit accountability mechanisms are needed to enforce rules. Accountability mechanisms should be enforced on-ledger where appropriate but can be enforced or complemented by off-ledger mechanisms.

4.2.4 Principle 4: Support transparency and openness

During a DLT system's lifecycle, the actions, decisions, and operation of the system should be transparent to DLT stakeholders to enhance trust. DLT systems should comprise mechanisms that allow stakeholders to observe and audit system dynamics.

4.2.5 Principle 5: Align incentive mechanisms with system objectives

Incentives in DLT systems drive the achievement of consensus among decision makers, the resolution of conflicts and decisions on the ongoing governance, design, and operation of systems. Incentive mechanisms in DLT systems play a key role in driving desirable behaviour across DLT users and other stakeholder groups. Incentive mechanisms should be explicitly designed to support system objectives.

4.2.6 Principle 6: Provide performance and scalability

If performance is not provided, the agility and maintainability of the system is affected. DLT systems should provide mechanisms to meet performance and scalability needs over the lifecycle of the respective DLT system. The use of DLT systems should be effective, efficient, and scalable while achieving system performance.

4.2.7 Principle 7: Make risk-based decisions and address compliance obligations

The lifecycle of a DLT system can pose specific risks, including jurisdictional challenges. Challenges should be assessed and treated appropriately in decision-making processes. DLT systems should seek

to set rules that ultimately induce self-compliance in order to reduce the risk of non-compliance with regulation.

4.2.8 Principle 8: Ensure security and privacy

Security serves the purpose of keeping confidentiality, integrity, and availability of the DLT system. The DLT system should provide appropriate security mechanisms. The safeguarding of privacy in DLT systems should be ensured. Privacy impacts should be considered. Depending on the task or process operated on a DLT system, related requirements should be addressed accordingly.

4.2.9 Principle 9: Consider interoperability requirements

Where DLT systems will need to work together with other systems, interoperability should be considered in the whole lifecycle of the system, especially at the design stage. A DLT system architecture should provide mechanisms to interoperate with other DLT and non-DLT systems with similar or different governance mechanisms in place.

5 Governance framework for DLT systems

5.1 Overview

This clause describes the governance framework for DLT systems. The framework for governance encompasses the decision rights, accountabilities and incentives associated with the governance of DLT systems. The differences between the governance of IT systems in general and the governance of DLT systems are discussed.

5.2 Comparison with other governance frameworks

Traditional approaches to governance of IT, for example as described in ISO/IEC 38500 and ISO/IEC/TR 38502, assume centralized governance. Such governance typically encompasses the effective, efficient and acceptable use of IT within the organization and is responsible for evaluating plans and proposals, directing policies and strategies and monitoring performance and conformance related to IT. An organization is not necessarily a company, enterprise, or government agency, but is assumed to be well-defined and be upheld by a clear source of authority. Boundaries on the scope and authority of a governing body are normally documented, for example, in a constitution, charter, or legislation. The implications of organizationally bound IT governance flow through elements and assumptions of these existing governance frameworks. These are commonly reflected in the role of conventional IT governance frameworks in defining and ensuring the implementation of IT strategy and business plans, the accountabilities of organizational management and boards, and the management of organizational risks including their relevant control treatments.

DLT systems differ from IT systems in general in that they involve distributed computing and are decentralized systems, where different nodes of the system are typically controlled by different organizations or individuals. In the context of governance, only organizations and individuals are considered as accountable entities. DLT systems can span organizational and jurisdictional boundaries. As a result, governance can span multiple organizations or individuals and therefore goes beyond the governance approaches of International Standards such as ISO/IEC 38500 and ISO/IEC/TR 38502. The relationship between the organizations and individuals involved with the DLT system is key and the governance framework for the system needs to address a series of critical questions such as:

a) What are the different types of DLT systems and how do they affect the establishment and execution of governance rules?

b) How do changes of the governing body over the lifecycle of DLT systems affect different DLT governance contexts?

c) Which stakeholder roles exist and how do they affect DLT systems governance?

d) How can risk, accountability, and compliance considerations be embedded in different types of DLT systems?

e) How can interoperability between DLT systems as well as between DLT systems and non-DLT systems be achieved and what are the governance implications?

To achieve effective governance of decision rights, accountabilities, and incentives, DLT systems governance should accommodate for multi-stakeholder, distributed governance, reflecting the decentralization typical of DLT systems.

5.3 Specific governance considerations for DLT systems

Governance of IT is defined by ISO/IEC 38500 as 'a system by which the current and future use of IT is directed and controlled'. ISO/IEC 38500 covers many of the aspects of governance that also apply to DLT systems.

There are certain characteristics and dependencies of DLT systems that require a different approach to governance of IT as described in ISO/IEC 38500. While the governance of IT systems of a centralized organization is a relatively mature field, the governance of decentralized systems such as DLT systems is less well understood. This document addresses the unique aspects of governing DLT systems that warrant the adoption of specific governance functions and characteristics.

Governance of IT as defined in ISO/IEC 38500 addresses responsibilities and accountability. Another definition for governance of IT is given in Reference [17]: 'IT governance represents the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT'. This definition encompasses three key dimensions of governance of IT: decision rights, accountability, and incentives. These dimensions are useful when considering decentralized systems that span across multiple organizations.

The essence of a decentralized system such as a DLT system is that the system is typically decentralized among a group of organizations or individuals. The governance of such decentralized systems is closely connected to the nature of the group and the means by which the group is bound together.

There are three types of DLT systems with different governance structures and associated processes according to their degree of decentralization. While permissionless public DLT systems are considered to be completely decentralized, DLT systems that are permissioned public or permissioned private share attributes of centralization, see Table 2. For example, the governing body of permissionless public systems can be a decentralized group of pseudonymous stakeholders without any explicitly declared organizational hierarchy. In contrast, the governing body in a permissioned public system can be one or more entities clearly identifiable and verified. Different forms of governance implementations in permissioned public DLT systems are imaginable, such as cooperatives, oligarchies, or associations that can have membership voting mechanisms to elect representatives or appoint decision makers with tenure limited to a fixed period.

The key dimensions of DLT governance are described in more detail in Table 1, based on a definition provided in Reference [18].

Table 1 — Governance dimensions of DLT systems

DLT systems governance	
Decision rights	a) The allocation of decision rights in a decentralized environment can be less apparent and explicit than in traditional centrally governed environments. DLT users and other stakeholders affected by DLT governance decisions are impacted by how these decision rights are allocated. b) Decision rights can be defined on-ledger or off-ledger, and explicitly or implicitly. Implicit decision rights provide flexibility but are less easily scrutinized. Explicit decision rights are embedded within the DLT system design itself or defined by external reference. c) Where decision rights are explicitly embedded within the DLT system design itself, the application of such governance is enforced by technology, having less reliance on institutional enactment for its operation. d) The allocation and explicitness of DLT system decision rights can evolve through the lifecycle of a DLT system. For example, they can start as implicitly centralized and evolve to explicitly decentralized as the DLT system matures. e) Decisions can be achieved through off-ledger or on-ledger consensus or through external rules made by stakeholders involved in the DLT system. f) Forking is the ability for stakeholders to separate a new code base of a DLT system in order to establish a new DLT system with different governance mechanisms or rules. While it represents an existential separation of a DLT system and therefore reflects a drastic governance separation, its availability as an option also serves as a motivation for stakeholders to achieve a consensus on otherwise contentious governance decisions. g) Decision rights can evolve over the lifecycle of a DLT system. For instance, they can be centralized and exercised initially by a small group and then expanded to a wider or different group of stakeholders.
Accountability	a) Accountability is based on identifiability of DLT participants, who bear ownership of specific outcomes and decisions. b) Accountability is specified in the network and delegated to and by the DLT system.
Incentives	a) Incentives in DLT systems play a key role in driving behaviour across diverse DLT participants and other stakeholders. b) Incentives encourage the execution of activities necessary for the ongoing operation and governance of the system. c) If incentives for participants and other stakeholders are misaligned, they can lead to behaviours that ultimately are to the longer-term detriment of participants or stakeholders, potentially jeopardizing the operation of the system. d) Incentives in DLT systems drive the achievement of consensus among decision makers, the resolution of conflicts and the taking of decisions regarding the ongoing governance, design, and operation of systems.

DLT users are not necessarily bound by existing organizational relationships, nor are they necessarily constrained by common contracts, commercial agreements or even jurisdictions. Governing such systems requires specific adaptations to accommodate for the potential lack of typical governance mechanisms and conventional sources of decision-making authority and accountabilities.

DLT users and other stakeholders organized in a decentralized or polycentric system will benefit from clearly specified decision-making rules, accountabilities, and incentive structures at each DLT systems lifecycle stage.

The nature of governance of DLT systems will also depend on the level at which the system will be governed, see Figure 1.

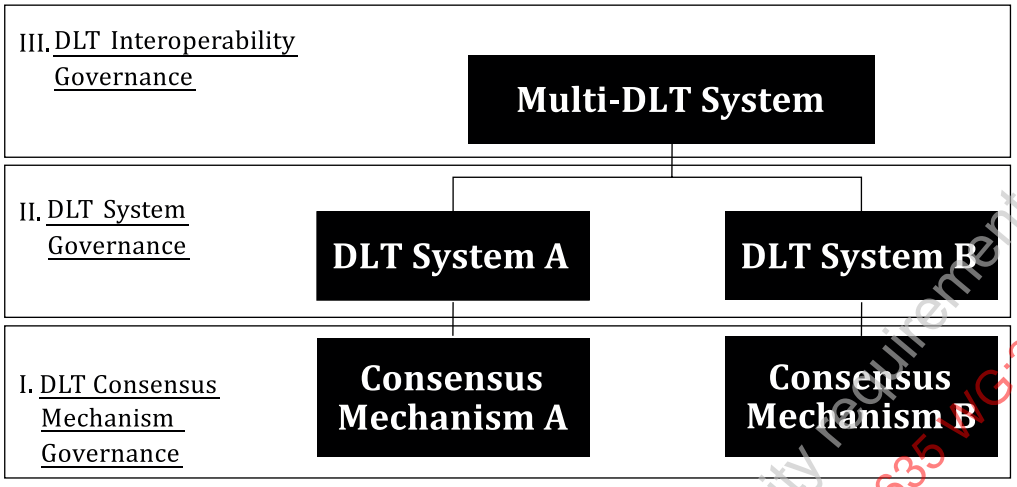

Figure 1 — Levels of DLT systems governance

For Level I, DLT Consensus Mechanism Governance, choosing a certain consensus mechanism, such as proof of work, proof of stake, or proof of authority, defines subsequent decision rights and incentives and thus determines the overall governance.

For Level II, DLT System Governance, governance of DLT systems is achieved through the application of on-ledger technically enacted governance mechanisms or through off-ledger governance that relies on supporting, sometimes implicit decision-making processes, accountabilities, and incentives. Level II governance dictates how DLT system decisions are made and how potential conflicts are resolved. On-ledger governance dictates that codified DLT governance rules will determine which participants are allowed to participate in such decisions, how disputes are resolved, and how voting mechanisms work to achieve acceptable consensus for specific decisions.

For Level III, DLT Interoperability Governance, inter-system governance, ensures the interoperability of DLT systems with other systems and broader non-DLT contexts.

In the context of DLT governance, it is necessary to distinguish between governance of DLT systems and governance through DLT systems.

a) Governance of DLT systems

Governance of DLT systems follows the logic of other socio-technical standards, that perceive technologies such as DLT systems as an operating object that need to be governed. This document largely follows that logic in developing guidelines for governance of DLT system for level II and III as illustrated in Figure 1. Following that view, the source of control ultimately resides outside the DLT system and a governance regime is enforced on it.

b) Governance through DLT systems

Governance through DLT systems follows the logic of algorithmic governance or approaches it from a techno-social perspective. Technologies such as DLT systems are perceived as an operating agent that is exercising governance. In Figure 1, once a consensus mechanism has been chosen and implemented, the algorithmic governance regime that comes with the consensus mechanism in level I governance is enforcing or dictating subsequent decisions and behaviours. Following that view, the source of control resides inside the DLT system and a governance regime is enforced through it.

While it is assumed that the notion of governance through DLT systems, sometimes referred to as algorithmic governance, is increasing in importance with the emergence of autonomous systems and machine to machine interaction, this document adopts a socio-technical view rather than a techno-

social view of DLT governance, with the source of control residing with human beings and legal entities rather than with technical entities.

Clarification of the source of control and authority in DLT systems is a key requirement for effective governance. This is particularly important due to the potential absence or otherwise diminished presence of decision-making authorities assuring the integrity of recorded transactions in these systems.

The decentralized nature of DLT systems can lead to reduced clarity of ownership of rights among DLT participants compared to more conventional, centralized systems (e.g. C-level management, shareholders, boards). Those who actively engage in governing DLT systems can therefore pay more attention to their needs as users rather than as owners of rights relevant to such decentralized systems.

5.4 Decision rights and decision-making

Decision-making is a key attribute of the governance of systems. The governance of DLT systems involves decisions such as decisions to fork, decisions on consensus rules that determine the on-ledger operation of systems, and decisions on the rights of diverse participants and how conflicts among them will be addressed.

DLT decision-making can take place on-ledger or off-ledger. When on-ledger, the decisions are governed by rules encompassing the decision rights and accountabilities embedded within the DLT system and executed accordingly. When off-ledger, decisions and authorities involve the application of either implicit or explicit governing rules, also encompassing decision-making rights and authorities. Implicit off-ledger governance has the disadvantage of not being as transparent to participants, while having the advantage of better protecting against risks and challenges not potentially foreseen by the on-ledger governance rules embedded within a DLT system.

Decentralized decision-making requires certain elements, techniques, and processes to be in place which differ from decision-making in centralized systems. A key characteristic of the decentralized decision-making relating to DLT systems is the use of consensus rules to arrive at decisions. Consensus rules articulate the criteria by which a decision will be approved into enforceability for participants in a DLT system. Consensus rules can take different forms. When embodied on-ledger, the DLT system itself provides the mechanisms for which decisions are formulated, defined, discussed, voted on and applied into operation. When off-ledger, other mechanisms such as legally binding obligations on specific participants are required to render decisions binding and operational in the DLT system.

5.5 Accountability

To increase transparency for current and future DLT users and other stakeholders, the responsibilities and accountabilities of parties within DLT systems should be declared and made explicit. This enables participants to understand how and where authority rests and reduces uncertainty for both DLT users and other stakeholders in assessing risks in relation to the operation of distributed ledger systems.

DLT systems that do not explicitly allocate accountability and responsibility for decisions include challenges that formalized legitimate decision-making authorities would avoid.

Without the declaration of location of authority for key operational and governance decisions, parties who do hold such control, often do so without formalized accountability, rendering participants unable to have even limited recourse to oversight and regulatory constraints in the event of governance failures. Examples include abuses of power, misappropriation of systemic assets, or decisions that do not align with the interests of significant proportions of DLT users. This presents challenges to stakeholders of DLT systems, leaving them with limited recourse to hold decision-makers with implicit authority accountable over DLT systems for decisions that go against the rules, principles or conventions of a DLT system, or the general interests of DLT users and other stakeholders.

DLT-based smart contracts and human-independent organizations also present accountability challenges. The novel nature of these capabilities presents challenges to conventional controls that regulators and governing authorities use to regulate the activities of individuals and organizations

to minimize systemic risks. Such control is typically levered on institutions and their executives over whom regulators and governing authorities exert authority over behaviour through the issuance of operating licences and the power to issue legal sanctions and penalties. When these control points are displaced by autonomous, decentralized governing entities, the resulting accountability vacuum challenges regulatory objectives and it is necessary to define underlying orchestration entities to support accountability within the uncertainty.

Smart contracts in distributed ledger system contexts allow unknown parties to transact with reduced risk of fraud and costs of third-party enforcement. In this manner, smart contracts provide an efficient means of addressing the costs and uncertainties associated with counterparty risks. Smart contracts conversely introduce key governance challenges in the form of uncertainty of their compliance with existing legal and regulatory frameworks and present challenges in enforcing legal rulings and sanctions as a consequence of their illegitimate or illegal operation. The logic that determines the actions of a smart contract, is embedded in its source code. Lack of visibility of this code can add further uncertainty to the allocation of accountabilities for these systems.

To address these challenges posed in DLT systems:

1) DLT providers should make visible to stakeholders the distribution of accountabilities for DLT systems. Ideally these accountabilities will be visible on-ledger. An alternative will be for off-ledger publication of accountabilities which is explicitly referenced on-ledger.

2) DLT providers should make their reporting on DLT systems available for independent auditing.

3) DLT providers should make DLT software code and documentation available to regulators or include resolvable mechanisms.

4) DLT systems should establish a dispute resolution mechanism for DLT participants, providers and broader stakeholders.

5.6 Incentives and incentive mechanisms

DLT systems present the risk of incentive asymmetries among stakeholder groups such as DLT users, DLT providers, and DLT developers. Incentive asymmetries can lead to system exploitation and economic and other imbalances among participants in a DLT system, ultimately leading to system failure.

DLT system incentives refer to any system design element that can influence the behaviour of participants. DLT system incentives can take a range of forms, from assurance of compliance with legal obligations to user-functionalities or economic incentives. Incentives can also take the form of encouragements for DLT participants and stakeholders to not behave in certain ways. These serve to discourage participants from actions that can adversely impact the longevity of the overall system or specific classes of participants.

DLT incentive mechanisms refer to specific implementations of incentives in DLT systems. On-ledger DLT incentive mechanisms manifest incentives into DLT systems using specific DLT constructs, including mathematical models in social science and computer science such as game theory-based reward mechanisms as economic incentives or incentives for supporting the validator needs. A key feature of many permissionless DLT systems is their use of on-ledger incentive mechanisms to motivate different stakeholder groups to behave in an intended way, assuring the system's ongoing stability and integrity.

Incentive mechanisms can also be off-ledger. These are often represented by conventional incentive constructs such as legally binding commercial obligations between parties, reputation maintenance within a community, and existing economic incentives.

DLT systems are by nature distributed. The increased complexity of participant relationships increases the inherent risks of misalignment of interests and incentives among participants. This occurs when participants are incentivized to behave in specific ways that lead to gain for themselves at the expense of other participants and the overall health and stability of a DLT system. If such an imbalance is

structurally allowed or otherwise entrenched within the dynamics of a DLT system, this can lead to sustained costs to one participant or class of participants that possibly warrant their departure from the system. If their presence is required by a DLT system for its continued existence, this in turn jeopardizes the longevity of the system itself.

When designing system incentives, it is important to consider the type of DLT system, since different types of systems require different incentives.

In permissionless DLT systems, participants can be anonymous or exempt of any formal relationships or contractual obligations. Such systems often rely on economic incentives to achieve consensus, manifested through reliance on-ledger tokens. In permissioned DLT systems on the other hand, participants are pre-defined, which means that incentives can usually be created through traditional means (e.g. legal contracts, creating efficiencies and business revenue). This also means that permissioned systems generally do not need native on-ledger tokens and can resort to existing enforceable associations between parties, typically manifested in off-ledger legally enforced relationships.

It is possible for some participants of DLT systems to have a blend of on-ledger and off-ledger incentives. In this case, visibility of off-ledger incentives should be provided to all participants to minimize the possibility of information asymmetries resulting in economic losses to less informed DLT participants.

When off-ledger incentive mechanisms are not possible or desirable (i.e. decentralized DLT systems), on-ledger incentive mechanisms are particularly important in implementing the governance of DLT systems. Effective on-ledger incentive mechanisms should enable the ongoing good governance of DLT systems and work in conjunction with any off-ledger incentive mechanisms that also exist among participants and stakeholders. To minimize risks of misaligned incentives, the on-ledger and off-ledger incentives of DLT systems should be declared and transparent.

6 Governance of different types of DLT systems

6.1 Types of DLT systems

From a governance point of view, DLT systems can be classified along two types of access dimensions (see Table 2). Access to transaction validation (by operating a DLT node) concerns the ability to validate transactions and maintaining control of installing updates of the protocol. In permissionless DLT systems, all entities have the right to validate transactions. Permissionless refers to the fact that there is no identifiable entity that owns the system and thus no one is legally entitled to exclude others from participating. In permissioned DLT systems, only entities that have been pre-registered have the right to validate transactions. Here, an entity that owns the system exists and thus can decide who is allowed to access the system to validate transactions and who is not.

The second form of access refers to technical excludability. Public DLT systems allow all entities to read data and propose new transactions. It is technically not possible to hinder access to the system. Private DLT systems only allow those pre-registered by a central authority to read data and propose new transactions. For the owning entity, it is technically possible to include or exclude entities to access the DLT system[18].

Table 2 — DLT systems governance types

	Permissioned	Permissionless
Public	Permissioned public Access is open to all entities – operating a DLT node requires authorization.	Permissionless public Access is open to all entities – operating a DLT node does not require authorization.
Private	Permissioned private Access is restricted for entities – operating a DLT node requires authorization.	Permissionless private Access is restricted for entities - operating a node does not require authorization. NOTE Not applicable from a governance point of view. A legally open to use good cannot be technically restricted in use. However, a permissionless DLT system's code can be used for developing a proprietary one, thus creating a permissioned DLT system.

Following that logic, permissionless or permissioned are dimensions that relate to some sort of ownership, while public or private refer to technical excludability. The source of control and authority is given priority over the technical excludability when it comes to governance. This is the reason why this document uses "permissionless public", "permissioned public", and "permissioned private" instead of "public permissionless" or only "public", as the latter ones are not specific enough to define governance types of DLT systems. These types result in various differences with regards to governance within that particular DLT system. From a lifecycle perspective, all these systems will still follow the lifecycle as described in 7.1, but the responsibilities and accountabilities of the various actors in the system can vary significantly per Governance Type. To better understand the different types of governance from the point of view of the nodes or validators and from the users of a DLT system, a specification of the functions in the operational stage of the lifecycle can be found in Table 3.

Table 3 — Types

	Functions for a DLT node			Functions for a DLT user	
Types of DLT system	**Read the ledger**	**Participate in consensus by validating transactions**	**Submit a new transaction**	**Read the ledger**	**Submit a new transaction through a DLT node**
Permissioned private	Pre-registered DLT nodes	Pre-registered DLT nodes	Pre-registered DLT nodes	Pre-registered DLT users	Pre-registered DLT users
Permissioned public	Any DLT node	Pre-registered DLT nodes	Any DLT node	Any entity	Any DLT user
Permissionless public	Any DLT node	Any DLT node	Any DLT node	Any entity	Any DLT user
Permissionless private [a]	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable

[a] Not applicable from a governance point of view, as the concept of permissionless private DLT systems is not well developed at this point in time.

Decentralization of decision-making processes means having a significant number of impactful decision makers, or voters. Resilience demands that decisions cannot be hijacked by a minority which, especially in permissionless DLT systems, requires a large fraction of active voters paying attention to each decision. Scalability in this context means potentially many decisions to be made at every voting round.

Decentralization of decision-making processes means also that one is operating without a central control mechanism, which is only the case in permissionless DLT systems and maybe for some permissioned systems in the operating stage. In the absence of a central operational control mechanism and the disappearance of trust procedures and authorities as proxies to generate trust in otherwise uncertain environments, concentrations of power should be avoided.

If the governing body accountable for the design and realization of a DLT system is organized centrally, a power concentration is created as it is the case in permissioned systems. Once the system is released, the DLT system then is a distributed execution of code that has been established centrally. For most, DLT systems are about decentralization and power dissemination, while another element in permissionless public systems is the possibility for everybody to participate in governance, referred to as inclusiveness.

In this document, DLT systems governance is structured along governance mechanisms and governance lifecycles for three different types, which are illustrated in Figure 2.

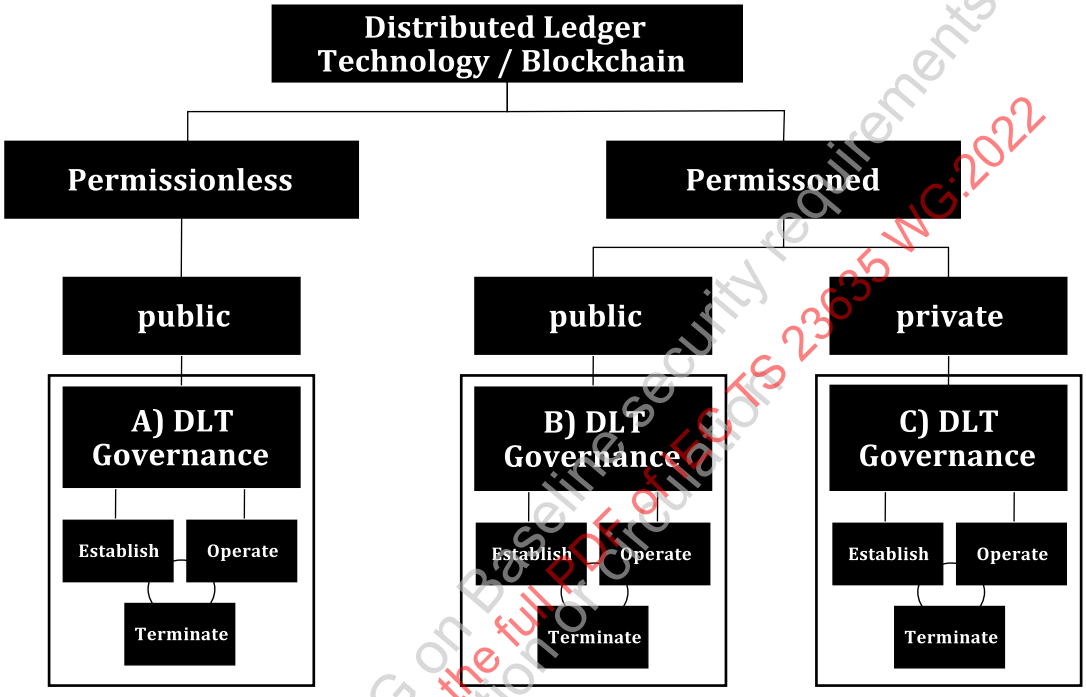

Figure 2 — Types of DLT systems governance

As an extension of the elaborations in Figure 2, the following characteristics of DLT systems are discussed, depending on the properties (permissioned/permissionless) and (private/public) and considering transaction validation and the openness or technical excludability. Distributed ledgers have many participating nodes, operating under a wide variety of organizational contexts that include:

a) Permissionless-Public: Where nodes are operated by separate parties (individuals or organizations) who not necessarily have shared interests and not necessarily recognize each other, nor be recognized by a clear source of authority.

b) Permissioned-Public: Where nodes are operated by separate entities (e.g. companies in the finance or supply chain industry) owned by, or responsible to, a shared top-level organization (e.g. an industry association).

c) Permissioned-Private: Where nodes are separate IT systems all owned and operated by a single entity.

Traditional approaches to governance of IT can be directly applied to type B and type C, although the detailed strategies, policies, and management systems for DLT systems can be different to those for conventional systems such as cloud systems or enterprise IT in general. Responsibilities and accountabilities can arise contractually in a sourcing arrangement, rather than through ownership by a single organization or consortium, but this kind of arrangement is accommodated by conventional approaches to governance of IT. For type A, traditional approaches to governance of IT can be effective to the extent that all parties jointly recognize a shared source of authority or governance body for their shared IT infrastructure.

6.2 Governance in permissioned systems

In traditional information systems implementations, access rules are defined by the owner or group of owners of the permissioned DLT system. While in case of a permissioned public DLT system the ledger can be decentralized, the access rules are defined by a central authority or a group, a consortium or committee of privileged users.

The conditions under which a user is given access to a DLT system can be that this user meets certain requirements (e.g. the user is a company that operates in a certain sector, is certified by a third party or adheres to certain capital requirement) or is co-opted or elected by other users or an authority. These access rules are entirely determined by the owner or group of owners that can be organized in any existing organizational form, in the establishment stage. In these DLT systems it is not possible to become a validating node or even reader of the system without consent of the owner or group of owners. All parties behind the system are known, identifiable and organizations behind permissioned systems are often set up as corporate structures, foundation structures or sometimes as systems similar to open-source development.

This also implies that accountability in the system is relatively easy to execute, and that such a DLT system can be maintained and even upgraded in a structured and organized manner. For permissioned DLT systems with known identities of all stakeholders, decision rights, accountability and incentive mechanisms should be clearly implemented.

As stated, governance in a permissioned private DLT system is similar to traditional IT governance approaches in hierarchically organized environments. A permissioned and private DLT system would be governed similarly to commonly used internal or shared IT systems by organizations. Since such a system is owned and operated in a hierarchical centralized way, with a single source of control and power clearly identifiable, the traditional governance approaches can be sufficient, and there may be no need to extend them with decentralized responsibility, accountability, and decision rights.

Within permissioned public DLT systems, elements of permissioned private systems as well as permissionless public systems can be found. Thus, those systems are typically referred to as consortium or hybrid systems. Where DLT users need permission to access the system, a privileged authority or governing body exists that can grant access. While that privileged entity has the rights to act on behalf of all DLT users, most permissioned public systems have distributed governance elements. The governing body owning the DLT system can decide to distribute decision power, accountability, and can provide incentives to the DLT network similar to permissionless DLT systems. The main difference in such a hybrid system would be that the privileged entity owning the DLT system can revoke the distributed decision-making at any point in time.

6.3 Governance in permissionless public systems

Traditional approaches to governance of IT assume that there is defined ownership as source of authority for a governing body that can act and be held responsible when necessary. However, in permissionless public DLT systems, there is no single source of authority.

During their lifecycle (see 7.1), permissionless and public DLT systems present unique challenges from a governance point of view. While the foundations for the governance are laid in the establishment stage, later changes and adjustments can be necessary, requiring soft or hard forks, which should be organized by on-ledger and/or off-ledger governance mechanisms.

In the establishment stage of a DLT system, the system architects need to design a governance system for the intended purpose. This could be done by a single authority or by a committee representing the community that later will use the DLT system. Once a governance system has been designed, it requires approval and adoption by the community before or at the time of launch. Approval can be done through actual adoption (users installing a wallet to transact with/through the blockchain), or through a voting mechanism that will legitimate the system proposed and officially validate its implementation, depending on the proposed process. Often, this is a balance between the proposal of the core developers and the adoption by the validators and full nodes, taking the incentives of different stakeholders into account.

In case the potential users do not adopt or perceive the governance structure they have adopted at a later point as unfavorable, they can fork and create their own new DLT system. Thus, forking is a governance instrument to deal with dispute in permissionless public DLT systems.

Permissionless public DLT systems are considered by many groups as a possibility to build participatory decision-making structures and decision-making processes into business models, thereby developing a new economic system. This is due to the attributes of DLT systems that provide validity, transparency, and auditability. This might call for revised or new forms of system maintenance, risk frameworks and ultimately governance, which possibly requires a reputation mechanism or another incentive structure.

Due to the high entanglement of permissionless public DLT applications and infrastructures, the governance of the infrastructure should take into account the governance of the applications built on top of it. In contrast to traditional IT governance, where it is possible to take an application offline, alter something and put it back online again, it is not possible in permissionless public DLT. When designing a governance system, it is of importance to take the type of application on the permissionless DLT systems into consideration. Types can be direct transactional (e.g. wallet) or conditional transactional (with smart contracts by identifiable parties behind it). Depending on the type, different governance approaches are applicable.

7 Governance throughout a DLT system's lifecycle and contexts

7.1 Governance throughout a DLT system's lifecycle

7.1.1 General

DLT systems proceed through a lifecycle of three core stages: Establishment, Operation and Termination, see Figure 3. The governance of DLT systems accommodates for the accountabilities, decision rights and incentives across these lifecycle stages. The nature of governance challenges and requirements can vary depending on the lifecycle stage of the DLT systems.

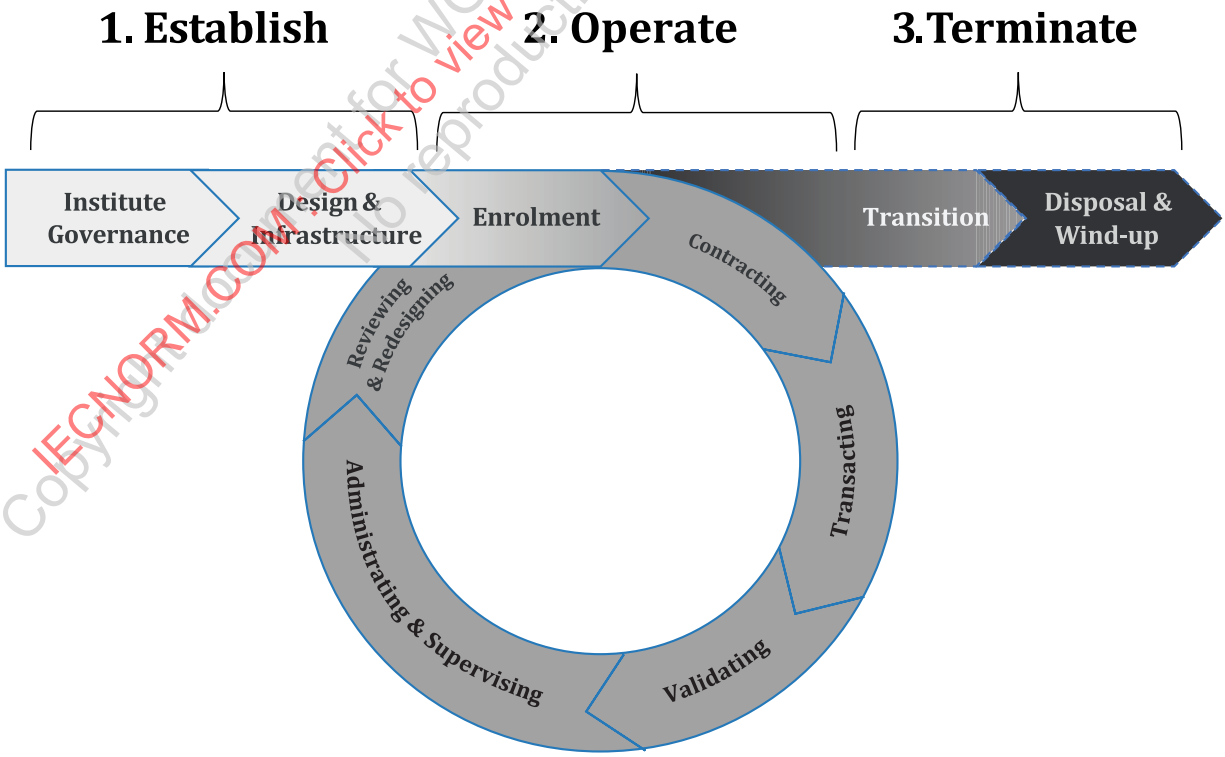

Figure 3 — DLT system's lifecycle

7.1.2 Governance in the Establish stage

During the establishment stage of a DLT system's lifecycle, the requirements and design of the DLT systems are formed, pilots launched and assessed, commercialization undertaken, and research conducted. It is during this stage that key governance functions and infrastructure are designed and implemented. These include:

a) the nature and type of governing body or structure;

b) the interoperability among DLT and non-DLT systems;

c) the compliance with legal and regulatory frameworks;

d) the existence and form of any DLT system constitution;

e) the dispute resolution mechanisms and procedures;

f) the extent and role of off-ledger governance;

g) the procedures and rules governing the operation;

h) the termination of a DLT system.

The making of these governance decisions is either implicitly or explicitly made by accountable parties, to whom accountabilities to these decision rights are either explicitly or implicitly declared during the establishment of a DLT system. Clarification of these decision rights and to whom or what they are vested in, will reduce uncertainty associated with the establishment stage of the lifecycle of the DLT systems.

Key decisions made during the establishment of a DLT system will define the governance of the subsequently rolled-out DLT system. Once these decisions are made by accountable parties, the next stage of governance decision-making in the establishment stage of a DLT system relate to the design of the DLT system and the infrastructure required to support the DLT system's operation. Governance decisions in this stage of establishment will involve how the DLT system will operate, the principles that will dictate its operation and how changes to the system will be agreed and applied once the system is operating.

7.1.3 Governance in the Operate stage

Once a DLT system has been established, it enters an operational stage of its lifecycle. Its core purpose and functions are executed according to the design it has been built to, and governed according to the decision rights, accountabilities and incentives that were put in place during its establishment. The governance of the DLT systems oversees several key functions during the operational stage of the DLT system, such as the enrolment of participatory rights for participants in the DLT system and the contracting rules associated with participation in the DLT system. All DLT systems operate within the context of legal and regulatory frameworks. DLT systems can provide guidance and on-ledger mechanisms for managing the operation.

Transacting among and between DLT users and off-ledger entities will be governed by rules and functions that dictate how these transactions will occur. It is recommended to identify rules and functions that are applicable to a given user's specific context. Furthermore, the validation of transactions is required to ensure that transactions performed on the DLT systems are deemed valid by the system and can be trusted as true and correct representations of reality by other DLT users. In the context of DLT systems, this will include validation, operating consensus mechanisms, consensus management, and enforcement of governance decisions. Administration and supervision of the DLT system occur through the course of its operation. This encompasses the actions involved in the ongoing operation of the DLT system. In the case of supervision, DLT systems operate within broader off-ledger contexts. DLT systems can provide on-ledger support for supervisory and administration functions with extraneous off-ledger supervisory functions.

The design and operation of a DLT system, as well as governance pertaining to its eventual termination should be designed during the establishment stage although it can be open to change during review of the ongoing operation of a DLT system. In this case, the governance of how this would occur will clarify where the accountabilities for such decision rights exist and how they will be applied and implemented.

7.1.4 Governance in the Terminate stage

At some point, DLT systems will enter a termination stage of their lifecycle. This stage will occur when the operational functions of a DLT system cease execution. In this stage, key governance decisions determine how data or assets of the DLT system are transferred, destroyed, or otherwise disposed of, and how the rights of participants are wound-up. The termination of a DLT system occurs within a broader external context. The governance of terminating a DLT system should explicitly support the external environmental interaction of the DLT system's termination. If it does not do so, the interaction of the DLT system's termination in the broader external context will be determined by the operation of extraneous off-ledger governance conditions and factors.

7.2 Governance in the DLT systems contexts

7.2.1 Overview of the DLT governance contexts

The different DLT governance contexts are shown in Figure 4.

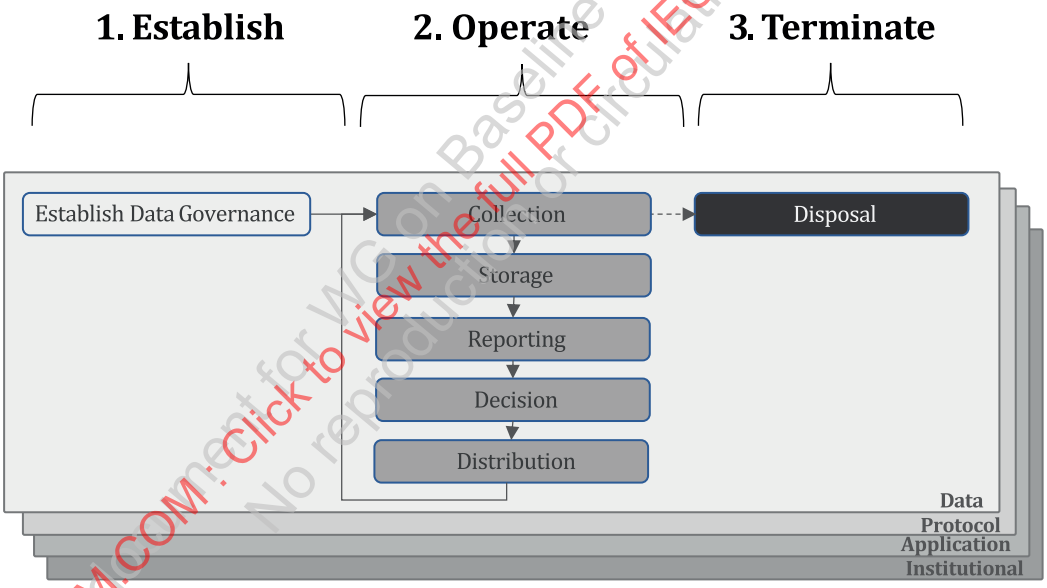

Figure 4 — DLT governance contexts

7.2.2 Data context

The data context comprises governance aspects of data aligned and adapted to the lifecycle stages of a DLT system.

During the establishment stage of a DLT system's lifecycle, the governance of data is defined. This includes how and which type of data will be defined, managed, and destroyed over its lifecycle within a DLT system. It will also determine governance of data as it co-exists and interacts with other DLT and non-DLT systems.

During the operation lifecycle stage of a DLT system, data is collected, stored, reported, incorporated into decisions, and distributed. The operation of a DLT system should anticipate how data will be governed in each of these functions.

During the termination stage of a DLT system's lifecycle, the governance of the DLT system should anticipate and guide the disposal of data, including its archiving or destruction.

7.2.3 Protocol context

During the establishment stage of a DLT system, the governance of a DLT system's protocols should be defined. This includes how DLT transactions will be defined and managed over a DLT system's lifecycle. Governance of DLT protocols during the establishment stage will also determine the interoperability of a DLT system's protocols with the protocols of other DLT and non-DLT systems.

During the operation lifecycle stage of a DLT system, DLT governance should define how protocols will operate and the rules governing their variation.

During the termination stage of a DLT system, the DLT system's governance should anticipate and guide how a DLT system's protocols will function. This includes guidance on how termination should be decided, executed, and validated.

7.2.4 Application context

During the establishment stage of a DLT system, the governance of a DLT system's application should be defined. This includes how decentralized applications are implemented, accessibility rights, and accountability. If applications are used by other DLT and non-DLT systems, accessibility rights and accountability need to be specified for this as well.

During the operation lifecycle stage of a DLT system, DLT governance should define how DLT systems' applications interact with each other and which governing rules for changes and maintenance of applications are necessary to support their ongoing use.

During the termination stage of a DLT system, DLT governance should envisage and guide how applications will be disposed of, destroyed, or transferred.

7.2.5 Institutional context

During DLT system establishment, the governance of a DLT system's institutional context should define how a DLT system co-exists and interoperates with specified organizational governance functions and operations. This will include how the governance mechanisms and structures of a DLT system relate to existing organizational governance functions, such as those performed by a board of directors and executive management. Alternatively, if no such relationship exists, this also should be declared explicitly.

During the operation lifecycle stage of a DLT system, governance of a DLT system within the institutional context should define how a DLT system's governance functions relate and interoperate with existing organizational governance functions, including how the decision rights, accountabilities, and incentives of DLT systems are exercised in relation to existing and relevant institutional ones.

During the termination stage of a DLT system, DLT system governance should define how it interoperates with existing institutional governance functions during the course of the system's termination, including on how decision rights, accountabilities, and incentives of DLT systems interoperate with institutional ones.

8 Roles in the governance framework

Responsibilities, accountabilities, decision rights, and incentives can be attributed to different roles within a DLT system, both in on-ledger and off-ledger contexts. Given the fact that there are many different setups for DLT systems, there is no single right way of allocating those attributes to roles within the system. Redundancies between roles can exist. The roles presented in the governance framework in Table 4 can be a single person/entity or multiple persons or entities grouped to accomplish the functions of the role. Not all roles might be relevant for all DLT types. Generally, DLT users utilize a system by means of an application or off-ledger code that interacts with the API, rather than directly

interacting with a DLT node. This is true for DLT users that are automated systems rather than human users, where the interaction would typically occur via an API offered by the DLT application.

Table 4 — Roles in the governance framework

Role	Accountability	Responsibilities and decision rights	Incentives
DLT governor This role governs the DLT systems as a whole and keeps the DLT systems able to execute the tasks for which they were established.	Achieve long term business model viability and continuity (economic, ethical, legal, and financial) of the DLT system.	— Set and maintain policies with regard to responsibilities and accountabilities in relation to: — Purpose and values of the DLT system — Licensing — Membership types and roles, rules for onboarding and exiting members, competencies, work division and access rights — Decision rules and conflict resolution (voting mechanisms) — Off- and on-ledger decision-making arrangements and protocols — role and powers of community figurehead — managing voting and forking — Incentives, responsibilities and accountabilities at all positions and roles — Consensus mechanisms — Nodes that can participate in the DLT networks - including the minimum-security requirements — Communication management — Communication with external stakeholders (if applicable) — Work with DLT providers; and — Work with DLT node operators to ensure monitoring and governance is enforced. — Arrange processes and structures for sponsorship and funding — Manage industry consortia, manage single corporate sponsor relation — Design and/ or approve compensations and incentive schemes for developers and other contributors	Increase of value of system tokens

Table 4 *(continued)*

Role	Accountability	Responsibilities and decision rights	Incentives
DLT auditor DLT auditors ensure that policy, governance and regulation are adhered to in DLT systems. They can work with operators, regulators, governors, etc.	Collecting and verifying evidence for audit to policies in DLT systems, signal deviations to relevant parties e.g. governor, administrators, others	— Set policies for audit activities on relevant perspectives and risks in both performance and compliance — Ensure the availability of instruments for auditing and reporting on DLT components — Report on auditing results — Engage in and support discussions on non-compliance — Propose solutions, support in enforcing corrective actions — Audits the DLT system	Increased token value Other benefits
DLT administra-tor DLT administrators perform specific administrative activities (in particular for security configuration).	Ensure full integrity of the DLT system	— Verify identity, authenticity and authorizations to users, oracles, smart contracts, wallets, and exchanges — Key management and privacy — Risk management and mitigation strategies — Manage role-based access to the DLT systems — Develop and manage privacy and security policies and protocols — Onboarding and exiting of users — Handling exceptions — Installing user applications	Increased token value Fees Other benefits
DLT developer There are two sub-roles for DLT developers - DLT application developers and DLT system developers	Ensure the continuity of the DLT system by continuously adapting the system to technical and business demands	— Manage community signalling processes for development policies and planning — Decide on development modularization — Design, create, integrate and maintain required code for all DLT components, e.g. smart contracts, API, data synchronization — Release software development kits — Design, create, integrate and maintain specialized equipment — Decide on build releases — Decide on test management — If applicable: manage in-company development teams — Manage incentives for developers and contributors	Increased token value Fees Other benefits

Table 4 *(continued)*

Role	Accountability	Responsibilities and decision rights	Incentives
DLT provider DLT provider is a role which can own and operate one or more nodes within DLT systems and DLT networks. Sub-roles include: DLT system operators, DLT Node operators, and DLT Application operators.	Ensure the business continuity and required technical performance of the virtual and physical elements that run the component of the DLT systems.	— Handle business requirements — Contribute to change decisions — Manage network connections and data synchronization — Manage life cycle: maintain build, test, deploy, run ledgers, smart contracts and consensus mechanisms in secure runtime environments, end nodes — Ensure interoperability — Decide on shards, light nodes, other configurations — Propose and /or decide on architecture and organization for DLT provisioning — Manage required competencies for continuity of the DLT systems, implementing system continuity. — Onboarding and exiting of users — Trouble shooting	Increased token value Fees Other benefits
DLT user This can represent an individual, organization, device, or system.	Ensure the continuity of the DLT system by using in a non-fraudulent way, thereby reinforcing the governance rules and their application.	— Uses services provided by the DLT system — Installing and configuring user applications — Use DLT user applications — Install client or application for interacting with a DLT system — Handling exceptions or failures — Observes and follows rules and does not engage in fraudulent behaviour — Reinforces the DLT system and its governance regime through its use — Engage in transactions that are subject to governance	Increased consumer rent Other benefits

9 Governance instruments

9.1 General

DLT system governance is performed through instruments internal to the protocol (on-ledger), external (off-ledger) and through the interaction between on-ledger and off-ledger. It is recommended to identify and document the instruments and the interactions between them in any system-specific governance policy to allow for transparency and aid accountability.

On-ledger governance instruments are written into the DLT protocols or executed by smart contracts. The governance instruments can be activated by on-ledger or off-ledger events. On-ledger governance instruments act according to their programmed logic and can be responsible for actions, but they are not accountable for those actions.

Off-ledger governance instruments are applied outside the DLT protocol. Typically, off-ledger governance instruments connect the protocol with legal entities and define decision rights, accountabilities,

and incentive structures. It is presupposed that off-ledger governance instruments enacted by legal entities comply with applicable regulatory frameworks, and appropriate legal obligations. Off-ledger governance instruments should align with on-ledger instruments and complement each other, where applicable. This can include a defined and formal protocol for which specific instruments or types of instruments are to be deployed within the DLT system. The governance of DLT systems is, to a large extent, determined in the establishment stage, including the selection of the consensus mechanism, as well as the rules and processes for developing and maintaining the DLT protocol over its lifecycle.

Each group of DLT stakeholders should be able to contribute to the governance of a DLT system through, where applicable, three main tasks based on ISO/IEC 38500:

a) Evaluate the current and future use of the DLT system and identify obligations and risks.

b) Direct prepare and implement policies, procedures and internal control frameworks to ensure that the use of DLT systems meets obligations and mitigates significant risk.

c) Monitor conformance of policies, procedures, and performance with the internal control framework operations to ensure risk mitigation and compliance with obligations.

Accountability for the effective, efficient, and acceptable establishment, operation, and termination of a DLT system remains with the governing body and should not be delegated.

9.2 On-ledger and off-ledger governance instruments

9.2.1 General

Both off-ledger and on-ledger governance instruments can be deployed within a DLT system, in order to achieve governance objectives. These instruments can be classified according to dimensions previously outlined in Table 1. Table 5 illustrates the characteristics of on-ledger and off-ledger governance instruments from the perspectives of Accountability, Responsibility and Decision Rights, and Incentives[19]. These characteristics are typical of the attributes required by DLT users to effectively design DLT systems.

The table is not exhaustive and overlap is likely to occur. In order for DLT systems to meet their intended objectives, various suitable combinations of instruments can be deployed. A DLT system can also deploy specific instruments that are not listed in Table 5. Any instruments used should be clearly documented so that entities can understand how the DLT system is governed.

Table 5 — On-ledger and off-ledger governance instruments

	Accountability	Responsibilities and Decision Rights	Incentives
On-ledger governance	— Identification — Access control — Confirmation — Auditing — Data conservation — Authentication	— Fundamental properties — Disposal rights — Access rules — Scope — Operation of consensus protocol	— Process execution model — Transaction process — Flexibility — Interoperability — Security — Operational alignment — Data validation