IEEE SA
STANDARDS
ASSOCIATION

IEEE Trial-Use Recommended Practice for Framework and Definitions for Blockchain Governance

STANDARDS

IEEE Consumer Technology Society

Developed by the
Blockchain Standards Committee

IEEE Std 2145™-2023

IEEE

IEEE Trial-Use Recommended Practice for Framework and Definitions for Blockchain Governance

Developed by the

Blockchain Standards Committee
of the
IEEE Consumer Technology Society

Approved 8 November 2023

IEEE SA Standards Board

Abstract: Provided in this standard is a common nomenclature and framework for describing blockchain governance across all use cases and contexts, including public, private, permissioned, permissionless, and hybrid. The standard is only normative regarding terminology. It is non-normative with respect to the design of particular blockchain protocols and systems. Where two terms are in common use for one concept, the standard shall define both terms and elaborate on any meaningful distinctions between them.

Keywords: blockchain, blockchain governance, design plan, framework, governance, IEEE 2145™

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the IEEE SA myProject system.[1] An IEEE account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

---

[1]Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2]Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has

---

[3]Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4]Available at: https://standards.ieee.org/standard/index.html.
[5]Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE recommended practice was completed, the Blockchain Governance Working Group had the following membership:

Savita Farooqui, *Chair*
Frederic De Vaulx, *Vice Chair*
Suri Jetty, *Secretary*

Les Aker	William Groah	Francis Mendoza
Nitish Bhardwaj	Kenneth Heung	Rajesh Murthy
Jacques Bikoundou	Hayley Howe	Pierre Marie Ntang
Wendy Charles	Wulf Kaal	Kyeong Hee Oh
Deniz Coskun	Tom Klein	Scott Perry
Thomas Cox	Chris Lambrou	Gustavo Prieto
Jack Crumbly	Kirsten Pomales	Rahim Rahmani
Soumya Kanti Datta	Langenbrunner	R. K. Rannow
Brian R. Dennehy	Mark Lesswing	Michael Solomon
Dave Dionisio	Vikas Malhotra	Sofia Tsekeridou
Tom Fuhrman	Mike Mcbride	Michelle Tsing
John Greaves	Jack Mccoy	Carol Van Cleef
	Denise Mccurdy	

The following members of the individual Standards Association balloting group voted on this recommended practice. Balloters may have voted for approval, disapproval, or abstention.

David Sebastian	Werner Hoelzl	Rajesh Murthy
Cardenas	Piotr Karocki	Bansi Patel
Xiaofeng Chen	Chris Lambrou	R. K. Rannow
Zhiman Chen	Daozhuang Lin	Diana Shi
Frederic De Vaulx	Weili Liu	John Webb
Jie Guan	Greg Luri	Yu Yuan
Shui Heung		Janusz Zalewski

When the IEEE SA Standards Board approved this recommended practice on 8 November 2023, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Sara R. Biyabani	Joseph S. Levy	Paul Nikolich
Doug Edward	Howard Li	Annette D. Reilly
Ramy Ahmed Fathy	Johnny Daozhuang Lin	Robby Robson
Guido R. Hiertz	Gui Lin	Lei Wang
Yousef Kimiagar	Xiaohui Liu	F. Keith Waters
Joseph L. Koepfinger*	Kevin W. Lu	Karl Weber
Thomas Koshy	Daleep C. Mohla	Philip B. Winston
John D. Kulick	Andrew Myles	Don Wright

   *Member Emeritus

Introduction

This recommended practice defines the terminology and framework for blockchain governance.

The framework describes the content and structure for Blockchain Governance Design Plan (BGDP), which becomes the controlling document for governing a blockchain solution. The plan defines the structure, processes, and policies necessary to support the objectives of the solution being governed. The plan can also be used to evaluate and assess blockchain governance for blockchain solutions.

The essence of the blockchain governance design process includes identifying the targets of governance for the blockchain solution (i.e., what components of the solution are to be governed), designing governance for each of these targets, and then creating a governance plan to inform and direct governance activities.

The targets of governance should typically include the technology solution, the corresponding ecosystem(s), and the solution development life cycle. Additional categories or targets of governance may be identified and included in the governance design.

Organizations that develop a BGDP using this recommended practice may include additional guidance for creating, managing, and updating the plan, taking into account the factors (e.g., organizational, risk management, environmental, political) that are specific to the solution being governed.

Contents

IEEE Trial-Use Recommended Practice for Framework and Definitions for Blockchain Governance

1. Overview

1.1 Scope

This recommended practice provides a common nomenclature and framework for describing blockchain governance for solutions across different use cases and contexts, utilizing public/private, permissioned/permissionless, or hybrid blockchains.

This recommended practice is only normative regarding terminology; it is non-normative with respect to the design of particular blockchain protocols and systems.

1.2 Purpose

The purpose of this document is to provide the terminology for describing, analyzing, and discussing blockchain governance across different blockchain protocols and systems, and to provide a framework and recommendations for creating blockchain governance design plan.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[6,7]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

---

[6]The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
[7]The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

1.4 Audience

This recommended practice is intended for the stakeholders associated with the design, development, operations, and evolution of a blockchain solution including the following:

— Those who conceive of an idea for a blockchain solution, and lead the creation of the solution (such as founders and key stakeholders).

— Those who wish to develop a BGDP (blockchain governance design plan) for a blockchain solution (governance designers working in collaboration with business and technical stakeholders).

— Those who design, develop, and operate the blockchain solution, and use the BGDP as the guide during these activities (business stakeholders, architects, software developers, network operators, communities).

— Those who evaluate a blockchain solution and associated governance design to make various decisions such as technology architecture and technology stack selection (architects), investment decisions (investors), whether or not to use or rely upon the blockchain solution, opportunity and risk assessment (consumers, relying parties), legal compliance (policy makers and enforcers).

1.5 Conformance to this recommended practice

A BGDP conforms to this recommended practice if that plan meets the reference outline provided in Clause 4.

2. Normative references

The following referenced documents shall be understood and used for the application of this document, and each referenced document is cited in text and its relationship to this document is explained. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ISO 22739:2020, Blockchain and distributed ledger technologies—Vocabulary.[8]

NISTIR 8202, Blockchain Technology Overview.[9,10]

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [11]

asset: A tangible or intangible object with an ascribed value.

blockchain: See ISO 22739:2020.[12]

blockchain application: A software application built using blockchain technology that delivers specific business functionality and usage.

---

[8]ISO publications are available from the International Organization for Standardization (https://www.iso.org/) and the American National Standards Institute (https://www.ansi.org/).
[9]NIST publications are available from the National Institute of Standards and Technology (https://www.nist.gov/).
[10]Available at: https://doi.org/10.6028/NIST.IR.8202.
[11]IEEE Standards Dictionary Online is available at: http://dictionary.ieee.org. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.
[12]Information on references can be found in Clause 2.

blockchain governance: The structure and processes of providing direction and/or control for blockchain targets of governance.

blockchain governance design plan: A document that describes expected blockchain governance for a blockchain solution.

blockchain network: A set of nodes that make up a blockchain solution.

blockchain node: A computing device that participates in a blockchain network through electronic peer-to-peer communications with other participating computing devices, and performs functions such as: (1) storing a complete or partial copy of the ledger; (2) executing the blockchain software, including consensus mechanisms; (3) executing on-chain code (e.g., smart contracts); and/or (4) participating in on-chain governance. *Syn*: node.

blockchain platform: The hardware, software, and infrastructure that implements blockchain technology and supports development and operation of blockchain applications.

blockchain solution: A system comprising technical capabilities, including hardware and software, that uses blockchain to provide business value.

blockchain solution lifecycle: The evolution of a blockchain solution through following phases: create, operate, evolve, and retire.

consensus: See ISO 22739:2020.

consensus mechanism: See ISO 22739:2020.

decentralized: A descriptive attribute of an entity or system that achieves, or for which the design goal is to achieve, a certain degree of the distribution of functions, decision-making and/or controls.

distributed ledger: See ISO 22739:2020.

distributed network: See NISTIR 8202.

ecosystem: A set of stakeholders.

governance administrator: One or more entities that facilitate implementation of governance decisions.

governance authority: The specific decision makers in a blockchain solution and how they are organized.

governance participant: A person, group, business, organization, or other entity that participates in blockchain governance.

governance target: Any component, entity, activity, or aspect of a blockchain solution, or the solution itself, that needs to be directed or controlled to deliver the blockchain solution objectives. Syn: target of governance, target.

governance token: A token that confers the right to vote on blockchain governance decisions through on-chain voting.

hard fork: See ISO 22739:2020.

incentive: A reward or penalty designed to encourage desired behaviors and/or to discourage undesired behaviors of parties involved in the creation, operation, growth, and governance of a blockchain solution to meet its objectives.

incentive design: The overall set of incentives that promote the viability and success of a blockchain solution.

network participant: A person, group, business, organization, or other entity that shares resources including data, storage, and/or computational power.

off-chain: See ISO 22739:2020.

off-chain governance: Blockchain governance in which decisions are made outside the blockchain solution.

on-chain: See ISO 22739:2020.

on-chain governance: Blockchain governance in which procedures to make decisions are encoded in the blockchain solution.

permissioned: See ISO 22739:2020.

permissionless: See ISO 22739:2020.

private blockchain: A blockchain solution that is accessible for use only to authorized users.

public blockchain: A blockchain solution that is accessible to any user without explicit authorization.

smart contract: See ISO 22739:2020.

stakeholder: A person, group or organization that is directly or indirectly involved in a blockchain solution.

soft fork: See ISO 22739:2020.

token: A type of asset used in a blockchain solution to confer rights and responsibilities to the holder.

3.2 Acronyms and abbreviations

BGDP	blockchain governance design plan
DAO	decentralized autonomous organization
DApp	distributed application
DLT	distributed ledger technology
KPI	key performance indicator
NFT	non-fungible token
P2P	peer to peer

4. Blockchain governance rationale

4.1 Overview

Governance is a particularly prominent area of focus for blockchain solutions, more so than for many other IT solutions. While any enterprise-grade IT solution requires deliberate and consistent management attention, there are certain characteristics of blockchain solutions that call for an even greater degree of strategic and operational engagement by the participating organizations.

Some of the unique aspects of blockchain that necessitate a new governance construct are described in 4.2 through 4.9.

4.2 Multi-stakeholder environment

Blockchain solutions are decentralized networked solutions that enable exchange of information and automation of business processes across organizational boundaries, which necessarily involve multiple stakeholders across an ecosystem that may have competing views and objectives.

Unlike traditional IT solutions that are created by a single organization for their own benefit, blockchain solutions are created by multiple stakeholders for the benefit of all, though the stakeholders may have different, sometimes competing interests. Identifying shared value and aligning the stakeholders toward a common goal is critical for the success of blockchain solutions. Blockchain solutions thus require a shift in thinking from a single organization's interests to the interests of the ecosystem as a whole, with multiple stakeholders working in concert to achieve and benefit from, the blockchain's trust and transparency features.

4.3 Shared resources

Enterprise IT solutions are traditionally procured, deployed, and operated by organizations to address their specific business needs. Blockchain networks, on the other hand, are the products of a community. Node operators join the blockchain network and provide computing resources to run the blockchain software and perform the blockchain network activities (e.g., transaction validations and recording on the ledger).

At the business level, participating organizations may also share information and data, contribute funds, and/ or offer other resources for creating and operating the blockchain solution for the collective benefit of the blockchain network participants.

4.4 Distributed ledger

A blockchain solution is based on the premise of using shared ledgers to exchange information and share data. Each participant can maintain a copy of the ledger and get real-time, tamper-resistant access to data shared by other participants. As the ledger is shared among multiple participants, data can potentially be added by any authorized participants, which will then automatically be synchronized between the other parties crossing their system boundaries. In order to gain value from the shared ledger, the data in the ledger needs to be useful and usable, which in turn requires common understanding and agreements on what data are shared and how, the data standards, risks and benefits, liabilities, and incentives.

4.5 Networked technology

Being a networked technology solution, the benefits of a blockchain solution may depend on the "network effect"—the concept that the value of a product increases with the number of users or participants. For a blockchain solution, the perceived value depends on the use case, user/participant roles, and nature of blockchain. Network participants may contribute to the network by sharing data or resources, running nodes, and/or participating in the network activities such as transaction validations, block additions etc., that benefits

every other network participant. Network participation and growth can be encouraged with effective incentive design. The incentive design should be delineated as part of governance design.

4.6 Decentralized control

In a decentralized multi-party system, no single party controls the operation of the blockchain network and ledger. The system operates mostly autonomously as the result of the node software running on the individual and independent peer nodes that comprise the network. "Control and operation" of the resource is the duty of the network participants, whether enterprises or individuals. The ledger is updated with consensus from the network nodes, providing visibility and transparency, leading to increased trust in the network. Although no single party controls operational processes, decisions still need to be made, and governance shall be defined. Consensus-based decision-making processes are often employed.

In contrast, private blockchains often utilize elements of centralized control, although the general need for governance remains the same.

4.7 Disintermediation

By encoding the blockchain protocol and consensus mechanism in executable code, blockchain solutions can remove the need of an intermediary to validate and record certain data, or facilitate transactions. Use of blockchain does not guarantee data quality, but data integrity; bad data in will result in bad data out.

This feature is further extended with smart contracts used for automating business processes. The rules of business agreements are encoded into smart contracts, which automatically execute these rules when corresponding predefined conditions are met.

Achieving disintermediation involves the following:

— Common agreements among the participants about the solution (protocol + smart contract) requirements

— The rules of engagement and accurate encoding of the agreements in the blockchain solution

4.8 Tamper resistance

With the use of cryptography, an append-only data structure, transaction validations and consensus-based updates, blockchain provides strong controls to help prevent unauthorized modification of the ledger data. These controls also apply to the smart contracts deployed on the blockchain, making them tamper resistant. The visibility of the smart contracts and data on the blockchain provides an additional deterrent to tampering.

While tamper resistance is generally a desired feature, it also means that the smart contracts cannot be easily modified. It thus becomes important to establish a proper code development lifecycle governance structure that requires stakeholders to work together and agree on the business processes to be encoded in the smart contracts, and that the smart contract code correctly implements the intent of the agreements.

4.9 Incentives and token economics

Incentives are a key blockchain design characteristic that promotes governed behaviors of stakeholders. Incentive design is often a critical component of blockchain solutions considering its decentralized network, need to engage multiple stakeholders, share resources, and gain shared value. Incentives are designed to promote desired behavior in support of creation, operations, and growth of the blockchain solution.

The business value gained from the solution in itself can be an incentive in some cases, especially in private blockchains. In public blockchains, token economics is often used to provide financial and other incentives to the network participants.

These characteristics demonstrate why a decentralized, collaborative decision making is critical for the success of a blockchain solution. Blockchain governance is needed for such collaborative decision making in a multi-party environment, and it differs from conventional IT management in both scope and methods.

While such a network may be initiated and led by the founders or creators of the blockchain solution, the blockchain governance design should address how the larger network may participate in the governance, rather than the founders and early adapters controlling the decentralized solution.

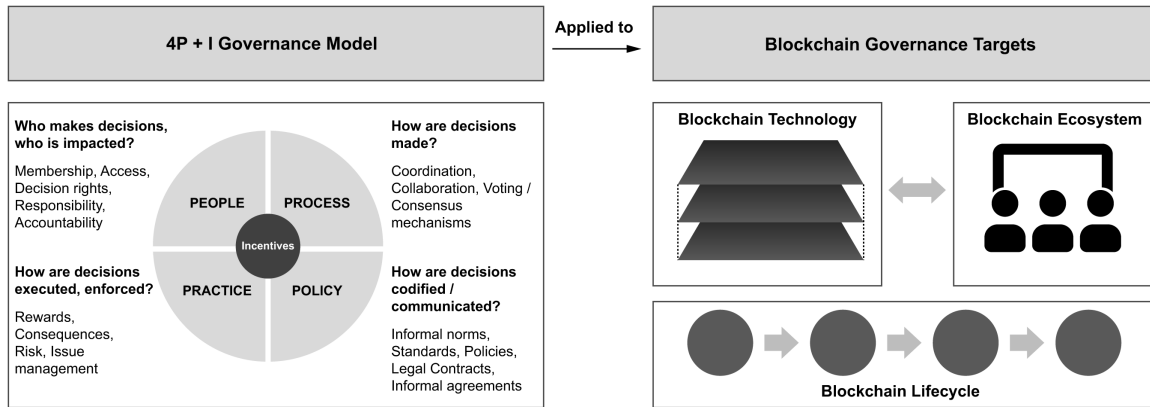## 5. Blockchain governance design framework

5.1 General

Blockchain governance provides direction and/or control for a blockchain solution by defining the structure and processes for making and implementing decisions that support the solution objectives. Blockchain governance design should take into consideration the blockchain solution's needs and objectives to help ensure that the governance design supports them.

A successful implementation of a blockchain solution requires governance for different components, entities, activities, or aspects of the solution—all working together to deliver the solution objectives. The blockchain governance process is designed, authorized, and implemented to govern specific solution components, with each component being referred to as a target of governance. This may include governance for blockchain protocols, network operations, software development, consortia or DAOs, among others.

A target of blockchain governance (or blockchain governance target) is any component, entity, activity, or aspect of a blockchain solution that needs to be directed or controlled to deliver the blockchain solution objectives. This practice recommends a modular approach for blockchain governance design that involves the following:

— Identifying the blockchain targets of governance. Blockchain governance should consider, at minimum, the high-level governance targets shown in the diagram presented in Figure 1. These are further elaborated in 5.2.

— Governance design for the identified target(s). This practice defines a governance framework to describe the structure of governance authorities, the processes for decision-making and coordination, the decisions made and their implementation. The governance framework is illustrated in Figure 1 and elaborated in 5.3.

Figure 1—Blockchain governance framework

Identifying targets of governance and their objectives should be accomplished prior to defining the scope, structure, and processes of governance.

For example, in the technology context, governance is needed for the blockchain protocol, the blockchain platform, and/or a blockchain application. In the blockchain ecosystem context, governance is needed for a consortium, working groups, or steering committees. Since blockchain is fundamentally a software solution, the creation, operation, evolution, and retirement of the software needs governance.
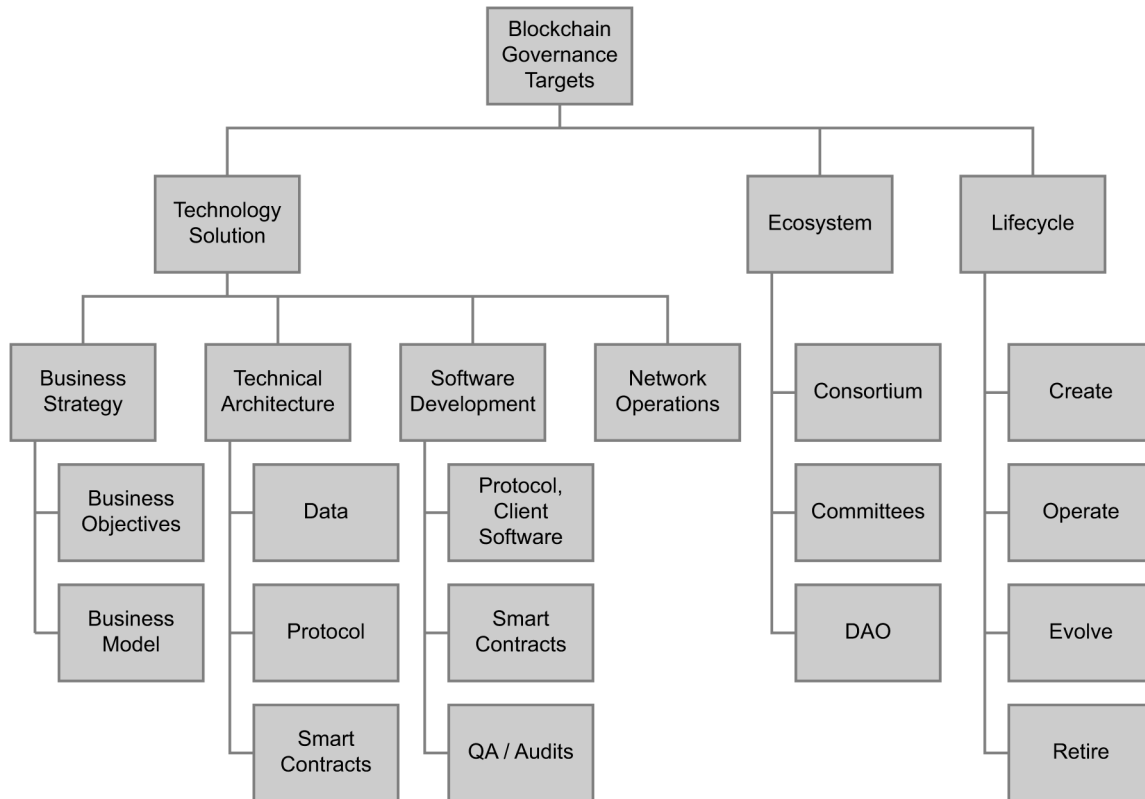
5.2 Blockchain governance targets

As the first step in blockchain governance design, this practice recommends identifying the blockchain governance targets. For an operational implementation of a blockchain solution in a multi-stakeholder environment, this practice recommends that blockchain governance should, at minimum, include the governance for the following governance targets:

— Blockchain technology solution

— Blockchain solution ecosystem

— Blockchain solution lifecycle

Within these minimum governance targets the user may also identify and create more detailed constituent elements for which direction and control is needed for the blockchain solution to meet its objectives and requirements. The governance targets should be selected to achieve a reasonable level of governance depending on the scope, objectives, and context of the solution.

Figure 2 shows possible governance targets within the high-level targets identified above. A blockchain solution should select one or more of these, and/or possibly other governance targets. The governance design at a higher level in the hierarchy may constrain the governance design at a lower level.

Figure 2—Example blockchain governance targets

The high-level targets are elaborated further in 5.2.1 through 5.2.4.

5.2.1 Blockchain technology solution

Blockchain technology solutions are created for the purpose of supporting business use cases and objectives. Governance of a blockchain technology solution is put in place to help ensure the chosen solution remains aligned with the business objectives throughout its life cycle. The business objectives themselves should also be clearly defined, along with the business model and business value for the participants.

The blockchain technology solution may also consider the following additional governance targets:

a) Business strategy: Govern business related decisions including business objectives, requirements, and business model.

   1) Given that a successful blockchain solution involves multiple stakeholders working across organizational boundaries, decision making for the blockchain solution should align stakeholders with shared objectives, based on common interests and motivations, align incentive schemes for continued engagement, and resource sharing.

b) Technical architecture: Govern the technical solution architecture and help ensure that it aligns with the business objectives and governance requirements/design.

   1) The technical architecture and selection of a technology stack for a blockchain solution should satisfy the business use case and business objectives. Depending on the use case, the solution may include creating a blockchain application, a set of smart contracts, a blockchain scaling platform, or a core blockchain platform, among others. A blockchain application itself may be a

distributed application (DApp) built on a DApp platform, utilizing smart contracts, and interoperating with other blockchains.

2) A data architecture should be defined that describes the data to be stored by the blockchain solution, where it is stored (on-chain or off-chain) and the data structures, addressing schemes, encoding standards, accessibility, confidentiality and availability requirements, cryptographic features (if any), relationships to other data items, and other requirements.

3) The selected technology stack may impose constraints on governance design. Thus, the business objectives, technical architecture and governance design may depend on each other and may need to be defined together in an iterative manner; for example, a business need for a private blockchain solution may constrain the technology choices, and the technology selection may impose constraints on governance design.

c) Software development: Govern the software development life cycle for the code involved.

1) Software development for a blockchain solution should follow industry best practices for a software development life cycle such as IEEE Software Development Lifecycle standards. Consider third party audit services, the QA/QC in a network environment and simulation of network growth to help ensure that the best practices are followed.

d) Network operations: Design the network to support the business and technical objectives and optimize network operations.

1) Focus on run-time operations of the network, updates to the node software and its deployment to the individual nodes (push or pull), and soft and hard forks.

5.2.2 Blockchain solution ecosystem

A blockchain solution ecosystem may include, but is not limited to, the following:

— Business stakeholders that share data and resources to create business value for all

— Users of the solution who may create and submit transactions, or access ledger data

— Technical stakeholders and communities involved in the creation and operation of the blockchain solution

— Investors and influencers who advocate and rely upon the solution

Each of these ecosystems taken individually or together may be considered as targets of governance in the context of a blockchain solution. The ecosystem may be organized using formal or informal structures such as consortiums, committees, working groups, communities, or DAOs.

Ecosystem governance is needed to help ensure that the ecosystem is created and operated to support the overall objectives of the blockchain solution. It also involves governance for the formal and informal organizations involved in the ecosystem, such as governance for the consortium or DAO.

a) The organizations that are likely to need governance and the purpose of organizational governance.

1) Consideration—Formal or informal organizations such as consortiums, DAOs, committees, or working groups should be created with specific objectives and goals to support the ecosystem objectives, including contributing resources to the ecosystem, and/or participation in ecosystem governance.

2) Common organizational structures include the following:

i) Consortia—wherein a blockchain solution is governed by a group of organizations, rather than one organization.

ii)   DAOs—in which stakeholders form communities to achieve common objectives.

iii) Committees, Working Groups—used to coordinate and facilitate blockchain solution-related activities.

b)   Organizational governance objectives include the following:

1)   Participate in and contribute to the ecosystem governance to meet the ecosystem objectives.

2)   Align organizational governance with the organization's objectives and ecosystem policies.

5.2.3 Blockchain solution lifecycle

In a distributed, decentralized deployment of a blockchain solution, the network participants contribute resources for the blockchain solution to function and deliver desired business objectives. In such scenario, the blockchain software code by itself may have little value without the network and associated ecosystem, and the success of the blockchain solution thus involves creation of the blockchain software, the blockchain network, and the blockchain ecosystem.

The blockchain solution may be initially envisioned by a single founder or a small group of founding members. Additional stakeholders may be onboarded over time (during solution development and/or after launch) to build and grow the blockchain network and the ecosystem. Blockchain solution governance design should consider this network and ecosystem growth, and address how the larger network may participate in governance processes to avoid concentration of decision-making power in the hands of founders and early adopters. An important purpose of governance is to sustain and increase decentralization since operational factors tend to work against decentralization in IT systems.

Blockchain project governance should coordinate and align software development, network, and ecosystem development to achieve the blockchain solution's business objectives. The development of blockchain software should still follow existing standards and frameworks for software development and appropriately integrate network and ecosystem development tasks as needed. Additionally, coordinated efforts should align software updates, network maintenance, and ecosystem engagement during the operations and maintenance phase of the solution life cycle.

The governance of the blockchain solution lifecycle includes the following:

—   Coordinating and aligning software and network development, and ecosystem engagement to achieve the blockchain solution's business goals.

—   Ensuring that the blockchain development follows industry standards for software development and aligns with the solution's business objectives.

—   Ensuring that the blockchain solution, network and ecosystem evolve to maintain collaborative, decentralized decision making to align with the blockchain solution's objectives.

The blockchain solution lifecycle includes the following phases; depending on the solution needs, these phases may themselves be unique targets of governance:

a)   **Create**: Align stakeholders toward shared business objectives; coordinate and align the software development, network, and ecosystem creation activities with the blockchain solution's objectives; facilitate agreements (data sharing, funding, strategy) creation.

b)   **Operate**: Coordinate and align the software operations, network, and ecosystem operations activities with the blockchain solution's objectives.

c)   **Evolve**: Coordinate and align blockchain solution evolution across the software development, network and ecosystem with the blockchain solution's objectives.

d) **Retire**: Coordinate and align end-of-life activities across the software development, network and ecosystem with the blockchain solution's objectives.

5.2.4 Other governance targets

In addition to the governance targets discussed in a) through d) of 5.2.3, additional governance targets may be needed to support the blockchain solution requirements related to the use case, industry sector, regulatory compliance, security and privacy requirements, interoperability, and use of tokens, among others. Some of these governance targets may span across the blockchain technology solution, the ecosystem and lifecycle. For example, a business requirement for regulatory compliance in healthcare or fintech industries may constrain the technology solution architecture, data sharing needs, impose certain restrictions on the implementation of the solution, and may also require (or not) maintaining identities of the ecosystem members.

Blockchain governance design should carefully consider the solution requirements and identify an appropriate set of governance targets.
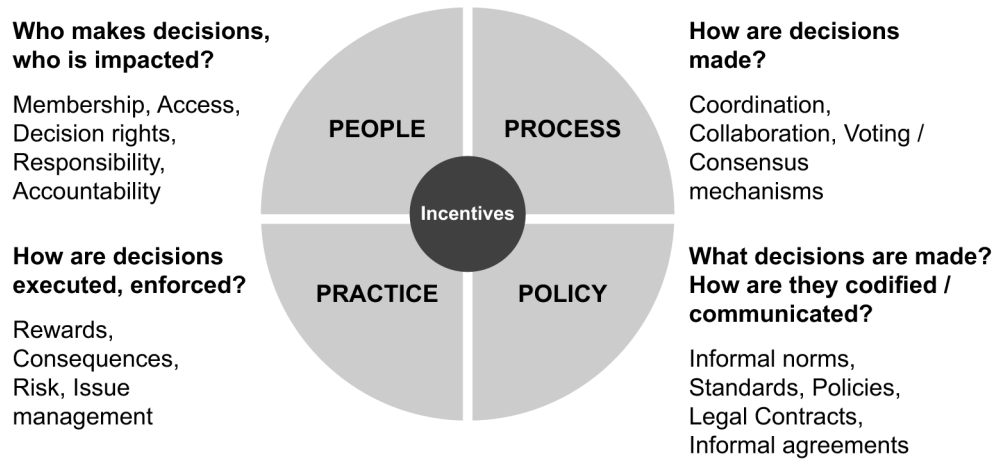
5.3 4P + I governance design framework

This standard introduces the "4P+I" governance design framework as a recommended practice for creating the blockchain governance design plan. The framework involves defining the structure and processes for decision-making and implementation, and aligning incentives with the system objectives.

At a high level, the 4P+I framework provides guidance for governance design for each target of governance by presenting a set of questions/considerations for the following design elements:

— People (governance structure): Who is involved in the process of governance, what parties are affected by governance, what are the roles and responsibilities of those involved?

— Process (governance processes): What are the processes for managing the membership, governance decision making, and/or managing the communication and coordination among parties? What other processes need to be defined?

— Policy (governance decisions/deliverables): What are the governance deliverables? How are they published and communicated?

— Practice (governance execution): How are the governance decisions/policies practiced? How is execution/compliance achieved?

— Incentives (governance effectiveness): What are the incentives/dis-incentives for parties involved (including the stakeholders, decision makers, administrators, community, end users)? How are the incentives aligned with the system objectives?

Figure 3 depicts the 4P + I governance design framework, incorporating the design elements discussed in this clause.

Who makes decisions, who is impacted?

Membership, Access, Decision rights, Responsibility, Accountability

PEOPLE

PROCESS

Incentives

How are decisions made?

Coordination, Collaboration, Voting / Consensus mechanisms

How are decisions executed, enforced?

Rewards, Consequences, Risk, Issue management

PRACTICE

POLICY

What decisions are made? How are they codified / communicated?

Informal norms, Standards, Policies, Legal Contracts, Informal agreements

Figure 3—4P+I governance design framework

The blockchain solution requirements have a strong influence on the governance design. These requirements may dictate who should be involved in decision making (e.g., centralized versus decentralized), the processes used for decisions making (e.g., direct democracy versus representative democracy), how the decisions are communicated, encoded, and enforced (e.g., traditional off-chain mechanisms versus on-chain algorithmic implementations using smart contracts, protocols, and/or consensus mechanism).

Subclause 5.3.1 provides more details on each of the elements of the 4P + I framework.

5.3.1 People

This subclause describes the people component of the 4P+I governance framework.

The following are examples of blockchain ecosystem members who may participate in governance, but the participants will differ for each project:

a) Ecosystem members (the governed): Those who are expected to follow, and/or are affected by the governance decisions (note that the decision makers and administrators themselves are also members of this group and are subjected to the governance decisions). The ecosystem members may be known or unknown, and their roles, responsibilities and privileges may be restricted or unrestricted. Governance design may consider following aspects:

   1) Identity: How member identity is managed (this may be handled by a separate governance plan)

   2) Roles and responsibilities: The roles that members may take, and the responsibilities associated with each. (The R-A-C-I framework—Responsible, Accountable, Consulted, Informed—may be useful for describing governance roles and responsibilities.) A roster of individuals and the roles they fill may be maintained, recognizing that the people and the roles themselves may change over time.

   3) Credentials and privileges: The credential(s) required to participate in a particular role and privileges associated with the role. For example, a consortium may have different membership levels based on their stake or investment, with associated voting rights, or privilege to participate in governance decision making.

b) Decision makers (governance authority): The specific decision makers, the structure of the decision-making team (if it is a team), how the members of the team are selected and assigned, and which governance model/type will be used: centralized, federated, decentralized.

c)   Decision administrators/enforcers (governance administrators): Those who facilitate, administer, and monitor the implementation of the decisions.

d)   Influencers: Those (by name or category) who have influence on the governance authority, administrators or processes for making and/or implementing decisions.

e)   Other parties.

The participants in governance should be organized in a way that best facilitates the governance functions. There are many ways to organize based on the type of blockchain, membership, use case, and other factors. The level of formality in the structure may also vary. Examples include consortiums, committees, working groups, and other forums.

5.3.2 Process

This subclause describes the process component of the 4P+I governance framework. This involves governance decision making processes, as well as communication and coordination processes to support the decision making as follows:

a)   Decision making structure: Decision making process depends on the structure of the decision-making bodies. The decision-making structures may range along the continuum of a single authority, to a committee to direct democracy. Depending on the use case and objectives of the governance target, appropriate decision-making structure may be chosen (note that the choice of a decision-making structure itself may be one of the governance decisions).

b)   Decision making process: If the structure of the governance authority is not a single authority, the members may use voting as the decision-making mechanism, and may need to determine the following:

   1)   What is the process for identifying and bringing issues to a vote (the proposal process)?

   2)   What are the criteria for eligibility to vote? (Criteria may include, for example, place in the hierarchy in an organization, investment of resources or funds, one department/one vote, one representative/one vote.)

   3)   Are weighting factors applied to votes, or are all votes individual and equal?

   4)   What is the voting method (e.g., direct, indirect, delegated)?

   5)   How is voting conducted?

   6)   How is a decision reached and finalized?

   7)   Is there an appeals process?

c)   Communication and coordination processes:

   1)   How are the members notified about proposals, voting events?

   2)   How do the members communicate and coordinate on proposal discussions, vetting prior to the final vote?

   3)   What is the nature of communication used to handle decision making? What are the service level agreements (SLAs) in timing and form?

   4)   How are decisions communicated to the stakeholders and others who are impacted?

      i)   Who is authorized to communicate on behalf of the governance authority and by what methods?

   5)   By what process or methods do indirect stakeholders or influencers have a voice in governance?

      ii)   What channels or forums are to be used, and under what rules or conditions (e.g., no payoffs for votes)?

5.3.3 Policy

This subclause describes the policy component of the 4P+I governance framework. In the context of the framework, the word "policy" is defined as the decisions required to govern the governance target, the formats for the related documentation, and mechanisms for communicating the governance decisions.

Required policies (content)—Different policies may be needed to help ensure that a blockchain governance target meets its objectives. The required policies may vary based on the type and objectives of the blockchain solution, and associated governance targets.

The following items are some examples of policies that may be needed. This list focuses on the content, rather than the format of the policies. This list should be updated for a specific project and governance target:

a) Membership policies (who can join, when, how, requirements for Know Your Customer (KYC), what they can do, if/how they can change roles, how can they leave)

   1) Data policies (what data are shared, ownership and control, liability management, data lifecycle, data interoperability, data standards—structure and semantics)

   2) Change management (how change is managed, change lifecycle—proposal, evaluation, vetting, updates, dissemination, deployment)

   3) Risk management (how risks are managed through its lifecycle, risk identification, evaluation, mitigation, monitoring)

   4) Dispute management (how disputes will be managed)

   5) Unintended effects, unanticipated issue resolution (how unanticipated situations will be handled)

b) Information dissemination (communication channel): The policy decisions need to be disseminated to those who are expected to follow, administer or enforce the decisions, or those who are affected by the decisions. The information dissemination process should help ensure that the appropriate audience is notified of, and provided access to the right policies (including content and format) in a timely manner, and that the integrity of the information is maintained. The following are some considerations for disseminating the governance decisions:

   1) The location(s) where the policies are published

   2) Notification to the right audience about the new or updated policies

   3) The access controls for the policies

   4) The versioning of the policy documents and the version control process

5.3.4 Practice

This subsection describes the practice component of the 4P+I governance framework. In the context of the framework, the "practice" focuses on the implementation of the governance decisions made in the "policy" section, including the administration and enforcement of those decisions. Some of the considerations to achieve this include the following:

a) Roles and responsibilities: Who is supposed to follow which policies? Who administers, supports, and enforces the implementation? What is the accountability associated with each role?

b) Policy implementation

   1) Training: How are the right policies communicated to the right roles? Is there a need to provide training and guidance to the parties involved to support the implementation? How the questions about the policy interpretation or clarity may be addressed?

2) Tools and technology to support policy implementation

   i) Are any systems needed to support the implementation of the policies? For example, will any tool or system be used to track risks and issues?

   ii) Will off-chain or on-chain mechanisms be used to implement policies? Which policies may be implemented using off-chain, traditional mechanisms, versus which policies may be implemented using automated on-chain mechanisms? For example, will some policies be encoded using smart contracts?

3) Success metrics/KPIs: How the success of policy implementation may be determined? What are the success metrics/key performance indicators (KPIs)?

c) Policy enforcement

1) Accountability: What mechanisms, tools, incentives (positive or negative) may be used to help ensure accountability for each role and party involved?

2) Incentives: How incentives may be used to support faithful implementation and adoption of the policies, as well as enforce accountability? Consider rewards and penalties to support this objective.

3) Tools and technology to support enforcement: Will any tools or automated processes including smart contracts, be used to enforce decisions and accountability?

d) Traceable metrics measurement/reporting

1) As the governance policies are implemented, effectiveness of governance should be measured against the established metrics for the blockchain solution success, success of the established policies, their implementation and enforcement. These measurements may be reviewed periodically to determine if any changes or updates to the governance design are needed to better support the objectives of the solution and each governance target.

2) Considerations for metrics measurement and reporting may include:

   i) Who is responsible for collecting and validating the metrics measurement data? What is the data analysis and reporting structure?

   ii) How are the measurements collected and processed? Manually or automatically from the solution data/logs? Can the data be validated?

   iii) What are the success criteria? Who decides the thresholds for success, considering that the definitions of success may be different for different stakeholders?

   iv) What is the reporting format (for example, interactive dashboards, reports etc.)?

   v) What is the frequency of reporting?

   vi) How will the metrics data be used?

5.3.5 Incentives

This subclause describes the incentives component of the 4P+I governance framework. The framework views incentives in a broader sense, not limited to the issuance of tokens or other rewards to incentivize certain objectives.

Incentives in the 4P+I framework refer to positive and negative incentives. Examples of positive incentives may include rewards, recognition and/or privileges. Examples of negative incentives may include penalties, consequences, and/or loss of privileges.

The incentives may also be direct or indirect, tangible, or intangible. For example, earning financial benefit by participating in a task is a direct financial incentive, while saving costs with improved efficiency may be an indirect financial incentive.

Incentives may be of different types such as:

— Financial (e.g., earning, saving, opportunity cost)

— Social (e.g., social media recognition, reputation, associated benefits)

— Regulatory/compliance (e.g., need to comply with laws, or the consequences of not doing so)

Incentives should be designed to support the objectives of the governance targets and to help ensure that the governance structure and processes are aligned with those objectives. The 4P+I governance framework considers incentives across the different components as discussed below.

a) Incentives for people

　1) Incentives for governing authorities, administering and enforcing authorities, members of the organizations, and other stakeholders to promote desired behavior that supports the governance target objectives.

　2) Incentives for other parties who may be indirectly involved in governance. Incentives may address, for example, encouraging the stakeholders to advance the objectives of the governance targets and those of the governing authority. Consider stakeholders such as:

　　i) Who may influence governing members and/ or their choices (e.g., lobbyists), or

　　ii) Who may be indirectly impacted by the governance decisions (e.g., consumers of an IT solution, peripheral stakeholders)

b) Incentives for processes

　1) Incentives for the decision-making processes to support the objectives of the governance targets and meet the governance requirements (e.g., inclusive governance should have inclusive decision-making process, and incentives should be designed to promote inclusive decision making).

　2) Prioritize where conflicts of interest may happen among the parties. Incentive design should take into consideration these conflicts and design incentives to arrive at consensus in spite of, and/or to address those conflicts.

c) Incentives for policies

　1) Incentives to invite, prioritize, and select policies that support and align with the success metrics and objectives of the governance targets. The goal is to avoid scenarios in which policies may not align with the overall objectives of the governance target even if the structure and processes are designed well.

　2) Incentives to help ensure that selected policies support the success metrics and objectives.

d) Incentives for practices

　1) Incentives to implement (execute, administer, enforce) and adopt the policies/decisions made.

6. Blockchain governance design plan reference outline

This clause provides a broad "reference outline" for a BGDP. The reference outline defines a canonical set of topics and considerations that should be addressed in a BGDP, with the recognition that the structure and content of any particular BGDP would be tailored to the particular needs of its business application. The BGDP may also include other topics.

The blockchain governance design plan outline is as follows:

1. Introduction
     1.1.   Purpose of the document
     1.2. Scope of activities
     1.3. Intended audience
2. Overview of the blockchain solution (Project)
     2.1. Purpose and objectives
     2.2. Context for the solution
     2.3. Key stakeholders
     2.4. Business model and business value
     2.5. Technical considerations
     2.6. Data considerations
     2.7. Governance considerations
     2.8. Risks
     2.9. Success metrics
3. List of selected blockchain governance targets
     3.1. Rationale for selection
4. Selected blockchain governance target (repeats for each blockchain governance target)
     4.1. Governance design inputs (Governance)
          4.1.1. Purpose and Objectives
          4.1.2. Scope
          4.1.3. Context
          4.1.4. Requirements/ considerations
          4.1.5. Success Metrics
     4.2. Governance design elements
          4.2.1. People
          4.2.2. Process
          4.2.3. Policy
          4.2.4. Practice
          4.2.5. Incentives

Each version of a BGDP based on this recommended practice should contain a title and a revision notice sufficient to uniquely identify the document. Revision information may include the name of the solution being governed, version number of the plan, date of release, approval signature(s), a list of pages that have been changed in the current version of the plan, and a list of version numbers and dates of release of all previous versions of the plan.

The introduction of a BGDP based on this recommended practice may describe the purpose, indicate the scope of activities, and identify the intended audience for the BGDP. A table of contents, and lists of the figures and tables in the BGDP should be included.

6.1 Introduction

Provide an introduction to the BGDP document. The introduction may include the topics such as the purpose and scope of the document, as well as intended audience. Additional topics may be added as needed.

6.1.1 Purpose of the document (why)

Provide information on the purpose of this document—what this document is about, and why it is needed.

6.1.2 Scope (what)

Provide information on the scope of this document. Describe what is included and what is excluded in the document.

6.1.3 Intended audience (who)

Provides information on the intended audience for this document.

6.2 Overview of the blockchain solution

Provide an overview of the blockchain solution, which may include a high-level description of the following subsections. Note that the overview included in this subclause should not be construed as an official statement of blockchain solution requirements. Reference to the official statement of solution requirements should be included in this subclause.

6.2.1 Purpose and objectives

Describe overall purpose and objectives of the blockchain solution, and the types of use cases/ features supported by the blockchain solution (some common use cases include cryptocurrencies, NFTs, financial services, track and trace, record keeping, provenance tracking, trade of digital (or digitized) assets among others).

6.2.2 Context for the solution

Describe the context for the solution. Identify any external factors that may impact the solution such as the following:

— Industry sector, jurisdiction-specific laws and regulations (such as HIPAA)

— Ecosystem culture, norms, standards, policies of the specific ecosystem

— Technical, social, financial, and other dependencies

6.2.3 Key stakeholders

Describe key stakeholders whose participation and engagement are necessary for the success of the blockchain solution. The key stakeholders may include creators, participating organizations, and customers among others. Identify the necessary roles and number of key stakeholders essential for the success of the solution.

6.2.4 Business model and business value

Describe the overall business model for the solution, including revenue or funding sources, operating costs, cash flow requirements, expenses, and financial liabilities. Describe how the solution will be funded during creation, operations, maintenance, and enhancements. Describe who has the ownership and control of the solution (e.g., all network participants in a public network—a decentralized autonomous organization, or a single party, a group or consortium in private networks).

Describe the financial accounting procedures and controls in place to verify accurate accounting and reporting. Describe financial auditing and transparency principles and practices that have been implemented. Describe who (by name or role), if anyone, has fiduciary responsibility over the treasury and stakeholder investments.

Describe the regulatory environment and the response of the governance authority to financial regulatory compliance. State whether the blockchain solution falls within a specific regulated category (bank, broker, dealer, money services business, nonbank mortgage originator/servicer, payday lender, etc.).

Describe the overall value proposition for the key stakeholders of the solution. For each of the identified roles of key stakeholders, describe associated value/incentives for that role. The value could be delivered in terms of:

— Investment and ROI

— Cost reduction and efficiency gain through increased transparency and trust

— "Opportunity loss" avoidance

— Social benefits

— Overall business value

6.2.5 Technical considerations

Describe the type of solution being created—if it is Layer 1 a blockchain technology platform, Layer 2 scaling platform, blockchain application platform, an application, or a service. Describe constraints on technology stack selection, if any.

Business objectives and use cases may dictate the technology platform selection, to ensure that the technology stack provides required features and functionality to meet the business objectives. The technology selection in turn may influence (constrain) the governance design.

6.2.6 Data considerations

Describe the specific data shared on the blockchain and the considerations related to the data that will require governance. Descriptions may include the following:

— The data structure, semantics, and metadata requirements.

— Any standards to be used or that need to be developed to define the data structure, semantics, metadata, and sharing envelopes for the specific data.

— Data ownership and access control requirements.

— Data validation and consensus requirements.

— Data dependencies including dependency on external data that may be stored off-chain or on other blockchain solutions. Describe the characteristics of such data and any relevant requirements.

6.2.7 Governance requirements/considerations

Solution requirements may sometimes explicitly include governance requirements (a requirement for a centralized vs decentralized governance, use of on-chain or off-chain governance etc.). At other times, governance design decisions may be derived from the solution requirements.

In order to design effective blockchain governance across different use cases and contexts, and across public, private, permissioned, and permissionless solutions, consider the following:

— Governance principles: In alignment with the principles of the solution being developed, the governance for the solution may need to abide by certain principles, such as a need to be participatory, inclusive, fair, and transparent, among others.

— Centralized versus decentralized governance, permissionless versus permissioned solutions: Depending on the business needs, a blockchain solution may be owned and/or controlled by a centralized or decentralized governance model, with some variation depending on the level of

29

decentralization supported. A blockchain solution may also be permissioned, permissionless, or hybrid depending on the use case to be supported.

— On-chain versus off-chain governance: A blockchain solution may include requirements for algorithmic, on-chain governance that automatically executes when given conditions are met, or a solution may require off-chain governance with human involvement and/or oversight for certain aspects. On-chain governance may be provided using the same chain or a different chain supported by an external, third-party application.

6.2.8 Risks

Identify and describe the risks associated with the solution, including estimates of likelihood and impact. Risks may include for example:

— Legal/compliance risks

— Liability risks

— Technology risks

— Security/privacy risks

6.2.9 Success metrics for the solution

Describe success metrics for the solution. The following list shows some success metric examples; however, each solution should select appropriate metrics aligned with the solution objectives.

a) Number of members

b) Number of nodes

c) Volume of data shared

d) Funds invested/return on investment

e) Engagement metrics (by the solution ecosystem members)

    1) Social media metrics (e.g., activity levels and sentiment analysis)

    2) Membership growth and retention rates

    3) Participation in governance

f) Number of cryptocurrency exchanges that list the governance token

g) Developer activity/number of developers

h) Integration with other applications (wallets, exchanges, products)

i) Revenue and profitability of the business platform

6.3 List of selected blockchain governance targets

This subclause should provide a list of targets of governance, along with their relationships with each other. A target of governance may be a component, task, activity, or aspect of the blockchain solution that needs to be governed. The governance targets may be related to other governance targets.

Governance may be defined for each individual governance target, or for a group of governance targets. If the governance targets are related in a hierarchical manner, governance may be defined at different levels in the

hierarchy to address specific objectives of governance at that level. Governance at one level may provide the context for governance at the lower level in the hierarchy.

Consideration: If targets are related in a hierarchical relationship, the list should reflect it.

6.3.1 Rationale

A brief rationale explaining the reason for selecting the target. Describe why this target has been selected for blockchain governance (e.g., the selection may be based on the blockchain solution requirements described in the previous sections).

6.4 Governance design

This subclause describes the inputs and outputs of the governance design for the selected target. This subclause should be replicated for each of the selected blockchain governance targets (listed in 6.4), with the names of the subclauses corresponding to the targets.

For each target of governance, create a subsection and describe the following:

— Governance design inputs

— Governance design elements

6.4.1 Governance design inputs

In order to meet the objectives of governance, governance design for each selected target should consider the following inputs:

— Purpose and objectives: Purpose and objectives of the target.

— Scope: Scope of the governance design for that target.

— Context: A set of external factors that may influence how governance is designed for a given target.

— Requirements/considerations (that might impact the governance decisions): Requirements and constraints of the target with regards to the blockchain solution that may impact of the governance design.

— Success metrics for the target: What are the metrics that would be used to measure the success of the target with regards to the blockchain solution?

6.4.2 Governance design elements

This subclause describes governance design elements of the blockchain solution in the 4P+I framework.

The governance design input for a particular governance target may determine if a centralized or decentralized governance is appropriate for the governance target. This means that the overall governance design plan for a blockchain solution may have both centralized and decentralized governance structures based on the governance target's needs.

Governance design for the selected target should consider the governance design inputs as discussed in 6.5.1, and follow the 4P + I governance design framework as discussed in 5.3 to define the following:

— People: Describes the stakeholders who are involved in or impacted by the governance of the target and the structure of organization of members that support the governance functions.

— Process: Describes the decision making, communication and coordination processes that will support the creation of policies for the governance of the target.

— Policy: Describes the types of policies, their implementations, and supporting activity necessary to implement governance.

— Practice: Describes the methods to translate the policies into activities.

— Incentives: positive or negative motivations to influence the designed governance outcome for the given target.

RAISING THE WORLD'S STANDARDS

Connect with us on:

Twitter: twitter.com/ieeesa

Facebook: facebook.com/ieeesa

LinkedIn: linkedin.com/groups/1791118

Beyond Standards blog: beyondstandards.ieee.org

YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060