Token

Transformative impact of disruptive technologies in public services

www.token-project.eu

D6.3
Governance Model (token-GovModel)

General information

Type	Deliverable (D)
Reference	D6.3
Version	0.4
State	Almost final draft

Owner	C. Harpes
Application date	19/12/2022
Classification	Internal (Public once approved)

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

Project full title

Transformative impact of disruptive technologies in public services

Contract No.
870603

Strategic Objective
SC6-TRANSFORMATIONS-2019

Project Document Number
SC6-TRANSFORMATIONS-2019-870603-WP6-D.6.1

Project Document Date
30.06.2021

Deliverable Type and Security
O - PU

Author
Carlo Harpes (itrust consulting / itrust consulting)

Contributors
Benjamin Hodzic (Infrachain / itrust consulting), Uwe Roth (Infrachain / LIST)

Document history

Version	Date	Author	Modifications
0.1	16/08/2021	C. Harpes	Creation
0.2	24/08/2021	C. Harpes	Integration of revisions and tailoring by Infrachain
0.2.1	24/11/2022	U. Roth	Add comments and contributions
0.3	25/11/2022	C. Harpes	Treat comments by U.Roth
0.4	19/12/2022	C. Harpes	Align to summary document D.6.3

This project has received funding from the European Union’s Horizon 2020 research and innovation program under Grant Agreement No 870603

Table of contents

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

List of figures

List of tables

No table of figures entries found.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

1 Introduction

1.1 Context

The objective of TOKEN is to leapfrog the adoption curve of Blockchain in public sector by creating tools supporting a community driven permissioned Blockchain hosting infrastructure. During the project, TOKEN was redefined to be Blockchain agnostic and support in particular the European Blockchain Services Infrastructure (EBSI).

In this document, we present the key principles and guidance related to the governance scheme. We intended to present the prerequisites for a community-driven Blockchain Platform as a Service (BCPaaS) with a view towards integrating it to any Blockchain environment. However, most component developed in this project will be supported in the same way as other open source tool, by the user community or the initial creator without a community effort specific to TOKEN.

One of the most often discussed benefits of Blockchains is that they can eliminate the need for a central authority. However, this is not entirely true, even for permissionless ledgers that anyone can access and conduct transactions or for applications and modules running on top of Blockchains. Blockchain modules do not appear out of thin air – they must be built and governed by code developers, engineers, and other decision makers who have been entrusted with key roles for the development of a BCPaaS. These developers are a de-facto central authority, and their composition and actions and underlying decisions may not be as transparent as the code itself. This raises and important question: Who, or what, is the legitimate governing entity of a BCPaaS, be it public or private? As greater accountability on all spheres of public life is demanded by civil society, decisions over who controls BCPaaS is of importance beyond the token project. This item even received more important during the project due to the concerns related to supply chain attack, a focus in the upcoming Network an Information Security Directive NIS2.0.

TOKEN added an interface in front of the used blockchain. Whoever manages that TOKEN API is the central authority to assume responsibility for the operation, independently of the creator of the API.

That's why TOKEN designed a Governance guideline able to be endorsed by Public Authorities across Europe if the have chosen the TOKEN API and want to maintain and scale it independently from its creator. This cornerstone aspect of the sustainability strategy is explicitly covered in WP6 and the results are presented in this report.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

1.2 Objectives

The purpose of this document is:

a. to present a governance model for use by a legal entity willing to use and maintain the BCPaaS platform after the TOKEN project;
b. to consider applying this governance model, mutates mutandis[1], by users of this platform when created a governance for their DLT system.

Governance is a 'system of directing and controlling'. The proposed governance model provides

a. principles for governance inspired by discussion on ISO standards and tailored to BCPaaS system governance and
b. an overview of the decision-making structure, comprising:
    1. the different committees overseeing the system's usage and development, and
    2. the design, implementation, operation, improvement and deletion of the main technical assets.
c. It considers interactions with external parties such as:
    1. Blockchain application providers wishing to deploy their applications by using the BCPaaS, and
    2. external regulators.
d. It helps to prepare agreements and organisational policies and procedure to be approved (or revised by different decision-making entities.

1.3 Enforcement and reading instructions

The use of the SIMPLE PRESENT tense or the terms 'MUST', 'MANDATORY', 'REQUIRED', or 'SHALL' in a statement means that the statement is considered a formal requirement.

The use of words such as 'SHOULD' or the adjective 'RECOMMENDED' means that there may be legitimate reasons to disregard the statement, but that the implications of such an exception shall be assessed and fully understood.

The terminology 'MAY' or the adjective 'OPTIONAL' means that the implementation of the statement is at the discretion of the implementer.

[1] with the necessary changes being made; with the necessary modifications; with such changes as are necessary to ensure congruence

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

1.4 Audience

This document shall be read and applied by project managers in public (and private entities) willing to design and operate DLT systems or applications that make use of the BCPaaS.

It should also by applied by all stakeholders in the continuing exploitation of BCPaaS.

1.5 Document structure

The remainder of the document is structured as follows:

- Chapter 2 deals with the DLT Governance principles from ISO 23635 and how thy apply to TOKEN.
- Chapter 3 describes a governance approach that can be applied, on the one hand, for maintaining the TOKEN API (and other tool) by a user community willing to add other features, further functional requirements, or product certification. On the other hand, it can also be applied by any project manager defined an organisation to maintain a DLT-based service and thus to ensure the sustainability of such a project.
- Chapter 4 illustration the relationship between actors and assets for a given application (PUC? Applied in TOKEN)
- Chapter 5 provide additional guidance related to certification as implementation of this important topic was not included in TOKEN project.

1.6 References

[1] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[3] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS directive).

[4] ISO/IEC 17000, Conformity assessment – Vocabulary and general principles

[5] ISO/IEC 17011:2017(en), Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies

[6] ISO/IEC 17021-1:2015, Conformity assessment – Requirements for bodies providing audit and certification of management systems – Part 1: Requirements.

[7] ISO/IEC 17065:2012, Conformity assessment – Requirements for bodies certifying products, processes and services.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

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

[9] ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems

[10] ISO/TR 23576:2020 Blockchain and distributed ledger technologies — Security management of digital asset custodians

[11] ISO/TS 23635:2022 Blockchain and distributed ledger technologies — Guidelines for governance.

[12] ISO/IEC 27001:2017, Information technology – Security techniques – Information security management systems – Requirements.

[13] ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management.

[14] ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

[15] ISO/IEC 38500:2015, Information technology – Governance of IT for the organization.

[16] ISO TC 307, SG6 Governance of blockchain and distributed ledger technology systems, Blockchain Systems Governance.

[17] FIWARE, Bylaws, https://www.fiware.org/foundation/bylaws/ downloaded 20221219.

1.7 Acronyms

AB	Accreditation Body
AP	Blockchain Application Provider
BCPaaS	Blockchain Platform as a Service
BO	BCPaas Owner (or BCPaaS implementation Owner, or simply Blockchain Owner) the Owner of the BCPaaS or the virtual or legal entity that will manage a DLT system (and use the service by the former BO).
BoD	Board (of Directors)
BP	Blockchain Provider
CB	Certification Body
CC	Certification Committee
CFC	Committee for Financial Control
CSI	Committee for Safeguarding Impartiality
DAO	Decentralized Autonomous Organization
DLT	Digital Ledger Technology
DoA	Description of the Action
GA	General Assembly

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

GDPR	General Data Protection Regulation
HO	Host Operator
IAF	International Accreditation Forum
LC	Legal Committee
P&AC	(Product and) Asset Committee
PII	Personally Identifiable Information
P&LC	Profit and Loss Committee
PUC	Pioneer Use Cases
QA	Quality Assurance
SLA	Service Level Agreement
WP	Work packages

1.8 Glossary

Note that "IS" stands for international standard and refer to the number of the ISO or IEC standard that created the definition.

asset	anything that has value to a stakeholder [IS22739]
blockchain system	system that implements a blockchain Note 1 to entry: A blockchain system is a type of DLT system. [IS22739]
consensus	agreement among DLT nodes that 1) a transaction is validated and 2) that the distributed ledger contains a consistent set and ordering of validated transactions Note 1 to entry: Consensus does not necessarily mean that all DLT nodes agree. Note 2 to entry: The details regarding consensus differ among DLT designs and this is a distinguishing characteristic between one design and another. [IS22739]
cryptographic hash function	function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally costly to find for a given output an input that maps to the output, it is computationally infeasible to find for a given input a second input that maps to the same output, and it is computationally infeasible to find any two distinct inputs that map to the same output Note 1 to entry: Computational feasibility depends on the specific security requirements and environment. [IS22739]
distributed ledger	ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism Note 1 to entry: A distributed ledger is designed to be tamper resistant, append-only and immutable containing confirmed and validated transactions. [IS22739]
distributed ledger technology (DLT)	technology that enables the operation and use of distributed ledgers [IS22739]
distributed system	system in which components located on networked computers communicate and coordinate their actions by interacting with each other [IS22739]

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

DLT governance	system for directing and controlling DLT systems including the distribution of on-ledger and off-ledger decision rights, incentives, responsibilities, and accountabilities [IS23635]
DLT node (or node)	node <distributed ledger technology> device or process that participates in a network and stores a complete or partial replica of the ledger records [IS23635]
DLT system	system that implements a distributed ledger [IS22739]
DLT user	entity that uses services provided by a DLT system [IS22739]
entity	item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence [IS22739]
governing body	entity that is accountable for the performance and conformance of the DLT Governance NOTE 1 to entry: This definition is inspired by the source below, but modified [IS23635]
hash value	string of bits which is the output of a cryptographic hash function [IS22739]
interoperability	ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged [IS22739]
ledger	information store that keeps records of transactions that are intended to be final, definitive and immutable [IS22739]
ledger split	fork creation of two or more different versions of a distributed ledger originating from a common starting point with a single history [IS22739]
nonce	number or bit string used once in a set of cryptographic operations Note 1 to entry: A nonce is often random or pseudo-random. It is commonly used to guard against replay attacks, where a message is captured and re-sent by a malicious actor. In some blockchain systems it is used to modulate mining during the generation of a new block and is stored in the block header [IS22739]
off-chain	related to a blockchain system, but located, performed or run outside a blockchain system [IS23455]
off-ledger	related to a DLT system, but located, performed, or run outside that DLT system [IS22739]
on-chain	located, performed, or run inside a blockchain system [IS22739]
on-ledger	located, performed, or run inside a DLT system [IS22739]
peer-to-peer	relating to, using, or being a network of equal peers that share information and resources with each other directly without relying on a central entity [IS22739]
permissioned	requiring authorization to perform a particular activity or activities [IS22739]
permissioned DLT system	permissioned distributed ledger system permissioned distributed ledger technology system DLT system in which permissions are required [IS22739]
permissionless	not requiring authorization to perform any particular activity [IS22739]
permissionless DLT system	permissionless distributed ledger system permissionless distributed ledger technology system DLT system that is permissionless [IS22739]
private DLT system	private distributed ledger system private distributed ledger technology system DLT system that is accessible for use only to a limited group of DLT users Note 1 to entry: Public and private categories apply to DLT users, and permissioned and permissionless categories apply to DLT users and those entities that administer or operate the DLT system. [IS22739]
public DLT system	public distributed ledger system public distributed ledger technology system DLT system which is accessible to the public for use [IS22739]

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

shared ledger	distributed ledger in which the content of ledger records is accessible by multiple entities [IS22739]
smart contract	computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger Note 1 to entry: A smart contract can represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction. [IS22739]
timestamp	time variant parameter which denotes a point in time with respect to a common time reference [IS22739]
token	digital asset that represents a collection of entitlements [IS22739]
transaction	smallest unit of a work process, which is one or more sequences of actions required to produce an outcome that complies with governing rules Note 1 to entry: Where appropriate, transaction is understood more narrowly, as the smallest unit of a work process related to interactions with blockchains or distributed ledgers. [IS22739]
trust	degree to which a user or other stakeholder has confidence that a product or system will behave as expected by that user or other stakeholder [IS22739]
wallet	application used to generate, manage, store or use private and public keys Note 1 to entry: A wallet can be implemented as a software or hardware module. [IS22739]

2 Governance principles

This chapter is inspired by ISO DTR 23635-1 : [8] and indicates how the customers governance principles are supported or reflected by the token platform.

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.

There are no users who access the services, but applications. For example, the developers of a PUC register their application at the TOKEN platform and receive an access token to access all services. From the application point of view, only the PUC platform accesses the services, not the users of the PUC. This access token is not an identity that is known by the blockchain. The TOKEN Platform accesses the blockchain, likely with its own unique identity. And even if the blockchain is managed inside a consortium as a permissioned blockchain with several nodes, there is no need for specific identifiers that act on the blockchain, apart from the TOKEN platform.

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.

There is no decentralize decision-making for the governance of the TOKEN services. Services like stamping, storing, and messaging do not require a decentralized decision. Decisions about the evolution of a TOKEN platform will likely not be decided by the use of the underlying blockchain, because the most relevant changes are those of the TOKEN APIs which do not necessarily use a blockchain in the backend.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

2.3Principle 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.

This principle focuses also more on open-source consortia and the ownership of IP as well as decision-making rights. Similar to Principe 2, this will likely not be based on a decentralized decision making that uses a blockchain. These elements have be defined in the TOKEN consortium agreement. In case they allow parties outside the consortium to contribute to the codebase, after the project has ended, the initial IP holders should still be in control of the code, e.g., decide on what is added and what not.

2.4Principle 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.

There is no transparency required for the TOKEN service and there are no actions, decisions, and operations that require this. Everything is behind the API. Users do not even need to know what Blockchain is being used. They will not have access to the permissioned blockchain or in the case of public blockchain will not know which transactions originated by TOKEN. Thus, the required transparency relates to the underlying blockchain, not the token platform, which, however, is open source to a large extent.

2.5Principle 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.

Since the TOKEN services are blockchain agnostic, this principle was not considered for the TOKEN platform.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

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.

If the TOKEN service is provided based on payments, it is the duty of the managers of the platform to deliver the requested service level, even if the codebase is open source. There will be no decentralized community that manages that platform.

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.

The TOKEN project developed guides to audit compliance (GDPR, NIS…) and applied them in POCs. These tools could be used by any TOKEN customers to assess compliance and could be provided as input for the company's risk-based decisions framework.

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.

Security and privacy are only marginally important for BSPaaS but relevant for the customer using the service. The stamping service has no privacy issue. The anchoring and streaming service require the use of encryption to protect privacy, but main aspects such as keys management is outside the service.

In general, security and privacy shall be ensured by the operator of the platform, not the manufacturer The TOKEN project did not foreseen to create a certified product for which a

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

certification needs to be maintained if changes are applies or if new risks appear. That's why the customer should follow an ISO 27001 approach when managing the operation of process with SW testing, system security monitoring, etc. Review templates for GDPR, 27701, and 27002:2022 have been prepared by TOKEN.

2.9Principle 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.

The BCPaaS is blockchain agnostic. However, the BCPaaS user should consider interoperability and migration to a different blockchain in his project conception.

For the TOKEN services, as it is blockchain agnostic, the underlying blockchain can be replaced with whatever is preferred. But once decided on one blockchain, the adding of additional blockchain into the running platform will likely not happen. And the transfer of data from one blockchain to another will be hard to achieve. Nevertheless, this principle asks DLT BCPaaS users to address these questions in the design phase.

Important to highlight that FIWARE technology related to Blockchain, Digital Identity, Verifiable Credentials, Wallet and so on is aligned with EBSI. Any application using Canis Major is already blockchain-enabled in an EBSI-compatible way. FIWARE has also put them in line with the European Strategy as key for sustainability.

2.10 Principle 9: Consider interoperability requirements

Where open source 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. An open source system architecture should provide mechanisms to interoperate with other open source and not open source systems with similar or different governance mechanisms in place.

The BCPaaS is blockchain agnostic. However, the BCPaaS user should consider interoperability and migration to a different blockchain in his project conception.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3 Governance of a DLT system (or a part of it, such a BCPaaS) - Model

Governance is a 'system of directing and controlling'. In this chapter, we explain how Token recommends open source system implementors to direct and control its different activities.

The open source implementor in this chapter is supposed to be a[n] [non-profit organization / economic interest grouping / public entity], called BCPaas Owner (BO). It may also be a[n] [non-profit organization, an economic interest group, a public entity...], which would need some obvious tailoring to the suggestions given here.

This model leaves room for several implantation options to be decided by the owner of the governance: sometimes it makes sense to create a dedicated legal entity for a given function, sometimes a loose coordination comity with agreed rules is good enough. The latter is often applied in open-source communities.

The so-called TOKEN governance model is spread out over multiple governance bodies and committees, within a specific context and shall be tailored to the existing governance culture. In this section, for each such entity, we indicate its:

a. responsibilities sorted by its duties to:
    1. assure,
    2. communicate,
    3. direct,
    4. evaluate, and
    5. monitor;

b. members, indicating how members are selected, for how long;
c. main activities;
d. decision taking, indicating how decisions are taken in case of diverging opinions;
e. performance, indicating deliverables, frequencies, and financial aspect of the operation.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

These entities are

1. the General Assembly,
2. the Board,
3. the Committee for Safeguarding Impartiality,
4. the Committee for Financial Control,
5. the Legal Committee,
6. the Certification Committee,
7. the Profit and Loss Committee and the
8. Product and Asset Committee.

Each committee, except for the Committee for Safeguarding Impartiality and the Committee for Financial Control, should be chaired by a member of the Board.

The following figure explains which entity elects, nominates, or validates the nomination of which entity. The relevant entity then reports in the inverse direction.

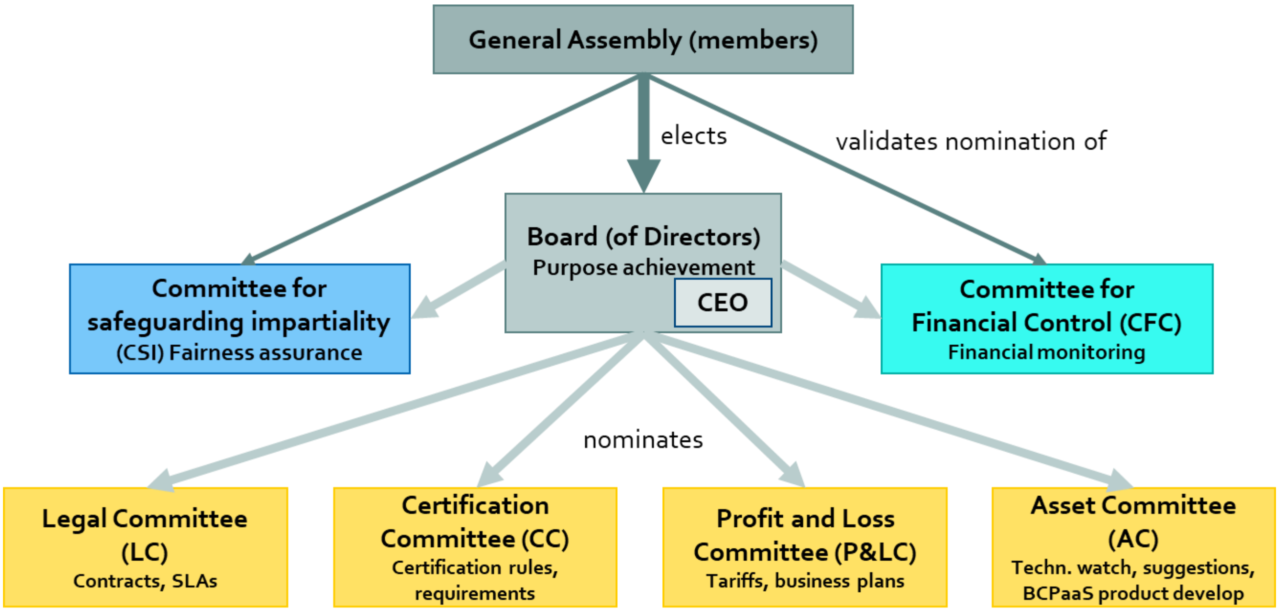
General Assembly (members)
elects
validates nomination of
Board (of Directors)
Purpose achievement
CEO
Committee for safeguarding impartiality
(CSI) Fairness assurance
Committee for Financial Control (CFC)
Financial monitoring
nominates
Legal Committee (LC)
Contracts, SLAs
Certification Committee (CC)
Certification rules, requirements
Profit and Loss Committee (P&LC)
Tariffs, business plans
Asset Committee (AC)
Techn. watch, suggestions, BCPaaS product develop

Figure 1: Governance bodies and nominations

3.1 General Assembly (GA)

The General Assembly has the role and responsibilities defined in the bylaw/statutes (or Articles). It does not exist for all contexts. For contexts managed by:

a. a single organization, the top management acts in the roles of the general assembly;
b. a large number of stakeholders, each having equal right, they should constitute an ASBL or ad-hoe organization, and the meeting of all members acts as General assembly.
c. For economic interest group, the General Assembly is a meeting of representatives of all shareholders, each representative having voting rights proportional to his or her share.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

Typical articles related to the general assemble are given below.

GENERAL MEETING.

All members may attend a general meeting. Only founding members and effective members have one voting right.

Members may be represented at a general meeting by another member. Only a member or a physical person representing a legal person that is member may receive a power of attorney. An effective member may be represented only by an effective member and a member cannot get more than two powers of attorneys. The annual general meeting will be held within the six months from the closing of each financial year preceding any ongoing financing year, as set forth under the conditions of Article X. Other general meetings may be convened in accordance with Article X.

POWERS OF THE GENERAL MEETING

The general meeting has the broadest powers to make or ratify the acts which concern the BO

The following are reserved to the general meeting:

(h) modification of the articles of association;

(i) nomination, revocation and fixing the number of directors and auditors;

(j) discharge granted to directors and/or auditors;

(k) approval of the budgets and annual accounts;

(l) dissolution of the BCPaaS Owner (BO);

(m) exclusion of a member;

(n) application for the recognition of public utility status;

(o) any proposal of the board of directors of the BO, mentioned in the convening notice of the general meeting.

CONVOCATION.

The general meeting is convened by decision of the board of directors or upon the demand of one-tenth of its members.

All of the members are convened to the general meeting at least two weeks prior to the meeting. These convening notices may be sent by mail, fax, be delivered personally or to the member's residence, or by any other means of communication.

The agenda is attached to the convening notice. Any proposal signed by a number of the members equal to at least one-tenth of the members shall be included in the agenda.

PRESIDENCY - MINUTES.

The general meeting is chaired over by the president or by the vice president, and in their absence by a member designated by mutual agreement of the board of directors from among its members. If no member of the board of directors is present, the general meeting will by itself provide for a chairman. Until such designation, the chairmanship of the meeting shall be entrusted to the oldest person by age present at the general meeting.

The secretary or another person designated for this purpose by the president records all resolutions of the general meetings in minutes signed by two directors and included in the special register.

A copy of these minutes may be obtained at the registered office of the BO

Minutes are taken during the course of the general meeting or before the following meeting and signed by the president or, in the alternative, by the vice president of the said meeting.

This project has received funding from the European Union's Horizon 2020
research and innovation program under Grant Agreement No 870603

DECISIONS OF THE GENERAL MEETING.

Resolutions are taken by a majority of votes expressed whatever the number of founding or effective members of the BO present or represented at such a meeting is, except if more stringent provisions are provided by the law or the present articles of association.

AMENDMENT OF THE ARTICLES OF ASSOCIATION.

The general meeting may only validly deliberate on the amendment of the articles of association if the text of the amendments is indicated in the convening notice, and if the meeting meets with at least two-thirds of the members.

An amendment may only be adopted by a majority of two-thirds of the votes expressed.

However, an amendment of the purpose of the BO may only be adopted by a majority of three-fourths of the votes expressed.

If two-thirds of the members are neither present nor represented at the first general meeting, a second meeting must be convened at least two weeks prior the latter in the manner provided for in these articles of association. This second general meeting may validly deliberate, regardless the number of members present or represented, and adopt the amendments according to the majorities set forth in the above section, subject to the homologation by the Civil Court.

The dissolution of the BO and the related measures shall be decided at the quorum and majority conditions provided for the amendments of the articles of association (other than an amendment of the purpose).

3.2Board (of Directors) (BoD)

3.2.1 Responsibilities

The Board is responsible to:

a. assure
   - the achievement of the purpose for which the open source system was established,
   - the general economic and societal well-being of the open source system,
   - adequacy of expenditures and revenues to the established budget,
   - elaboration of internal regulation,
   - the overall commercial and technological strategy of the open source system;
   - the open source system marketing activities, in particular the search for new Aplication Providers (AP)s;
   - the development of an open sustainable ecosystem around a public, royalty-free and implementation-driven BCPaaS that will ease the implementation of new Blockchain use cases in the public sector and beyond.

b. communicate
   - the overall status of the open source system to the general assembly, including general strategy, legal and economic context, and high-level technical aspects,
   - in public to represent the interest of the open source system,
   - in courts in his role to represent the open source system in court;

c. direct
   - committees,
   - a secretary,

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

- any person, e.g. a CEO, to which daily management has been delegated,
- other external experts in line with the established budget;

d. evaluate
   - the overall economic performance of the open source system;

e. monitor
   - the behaviour of theopen source system, with feedback from the Product and Asset Committee,
   - the state of the global open source ecosystem, with feedback from the Product and Asset Committee,
   - the legal and regulatory landscape, with feedback from the Legal Committee.

These responsibilities are in line with the statutes (the following are tentative statutes to be reviewed and completed by a notary is case of creation of a legal entity, or by lawyer in case of agreements between BO members):

BOARD OF DIRECTORS - COMPOSITION AND APPOINTMENT.

[…] Except for the first directors appointed by the first general meeting held immediately after creation, apart from potential co-opting by the board of directors and without prejudice to the terms of Article 17, members of the board of directors are appointed for a term of two years by the general meeting and chosen among the effective members by the general meeting. The term of their mandate expires on the day of the annual general meeting at the occasion of which the accounts related to the financial year following the one where they were appointed will be submitted to the general meeting for approval.

The members of the board of directors who are legal persons appoint a permanent representative for the purpose of their representation at the board of directors, in order to ensure the continuity of their representation among the board of directors.

The board of directors may, in accordance with the terms it sets in a discretionary manner, entrust any physical person with the position of secretary, whether that person is a member of the BO or not.

MEETING OF THE BOARD OF DIRECTORS.

The board of directors shall be convened in writing by the president or the vice-president at least twenty-four hours prior to the planned date of the meeting. The president or the vice-president is required to convene a meeting upon the written request of two directors. The board of directors may only act if a majority of the directors is present or represented. If the quorum is not met at the first meeting, the decisions may be taken at a second meeting, irrespective of the quorum, if it has been indicated in the convocation notice of the second meeting.

Decisions are taken by the majority of the votes expressed, subject to what is otherwise provided for by these articles of association; if there is a tie vote, the president or, failing that, the vice-president, has the casting and deciding vote.

In case of emergency, as assessed by the president or, failing that, the vice-president, the president or the vice-president may submit to the directors a proposal for resolution by circular means to be signed by all directors.

All decisions are recorded in minutes signed by two directors and included in a special register.

POWERS OF THE BOARD OF DIRECTORS.

The board of directors has the power to perform all acts necessary or useful to achieve the purpose for which the BO was established, except for those acts which the law or the present articles of association reserve for the general meeting.

The board of directors is empowered to set up committees, including a strategic committee whose tasks may, among other things, include the elaboration of a strategic direction, governance and operating rules of the BO network and among which founding and effective members will be ex-officio members whereas associate

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

members may sit at the strategic committee only upon co-opting by the board of directors at the occasion of a meeting of the board of directors where half of its members are present or represented and by a simple majority vote of such present or represented members. The board of directors will determine the operating terms of each committee set up by it.

DAILY MANAGEMENT.

The daily management of the affairs of the BO as well as the representation of the BO, as regards the management, may be delegated to any physical person, whether that person is a member of the BO or not. he board of directors may also, on an ongoing basis or temporarily, grant powers or special mandates or determined tasks to persons or agents or committees created for the purpose set by it.

REPRESENTATION OF THE ASSOCIATION.

Legal actions, as plaintiff or defendant, shall be instituted or supported on behalf of the BO by the board of directors upon pursuit and diligence of the president or, in the alternative, the vice-president.

Acts which bind the BO, are signed either by two directors or by any person(s) to whom such signatory power is delegated by the board of directors.

DIRECTORS' LIABILITY.

The directors do not incur any personal liability for the commitments of the BO Their liability is limited to the execution of the mandate they have received and to the negligence committed in their management.

The mandates of the directors are unpaid.

END OF DIRECTORS' MANDATE.

The mandate of any member of the board of directors may be suspended or revoked at any moment by the general meeting. A decision to suspend or revoke a director's mandate must be taken during a meeting of the general meeting where half of its members are present or represented and by a two- thirds majority vote of the expressed votes. A suspension shall terminate if no dismissal decision is reached within three months following the suspension.

The term of a member of the board of directors ends:

(d) when the member (or the member he represents) ceases to be part of the BO;

(e) by resignation;

(f) by death or incapacity or, in case of a legal person, by the liquidation or pronouncement of bankruptcy of that legal person;

(g) at the end of his mandate.

RULES OF PROCEDURE.

An internal regulation may be submitted for approval to the board of directors by a committee created for that purpose, including the strategic committee. Amendments to such a regulation may be made by the board of directors upon advice of such committee, acting by a majority vote of those present or represented.

3.2.2 Members (often called Directors)

The members of the Board are named by the General Assembly (GA) to represent all shareholders and key shareholders.

Optional: A few members may be appointed by Governmental entities (to support the societal dimension.

They hold their position for 2 years.

They cannot be members of the Committee for Financial Control (CFC) or the Committee for Safeguarding Impartiality (CSI).

The Board is headed by a president and a vice-president.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

The Board appoints an Executive Director (CEO) and delegates daily management task to her/him.

BOARD OF DIRECTORS - COMPOSITION AND APPOINTMENT.

The board of directors of the BO is composed of xx physical or legal persons. A president and a vice-president are appointed by it among its members.

Optional provision of representatives of the 'public sector'. The board of directors sets itself the rules related to its functioning.

VACANCIES

In the case of vacancy during the course of a term, including that of the president, a director ad interim may be named by the board of directors subject to ratification by the general meeting. The director ad interim will, in this case, complete the term of the director he replaces.

Exiting directors may be re-elected.

3.2.3 Activities

3.2.3.1 Commercial

The following needs alignment with business plan of the organization (i.e., D6.2 for TOKEN)

The Board votes on the acceptance of new members.

To find and onboard new APs that make use of the open source system, the Board engages in dissemination and marketing activities. APs and applications may be suggested by any member of the BO.

The Board decides on the underlying blockchain and other service provided on which a service depends.

The Executive Director signs SLAs with those APs that wish to receive paying support services.

3.2.3.2 Governmental

The Board calls and organizes all meetings and elections involved in the governance of the BO, in particular: General Assemblies, elections of the Board itself, and all referenda required to validate certain Board decisions. Referenda are required to: confirm Committee nominations of the Committee for Safeguarding of Impartiality and the Financial Committee, confirm a governance change (e.g. the creation of a new committee or of a new rule), confirm the abandoning of a certain blockchain technology.

The Board nominates the members of each of the committees.

The Board votes on:

- taking the initiative to temporary or permanently exclude a Member (to be declared by the next General Assembly);

In case of emergency, e.g. data breach or fraudulent activity, the Board can decide in the interest of the BO, to stop activities immediately. If this happens, the Board calls for an immediate Extraordinary General assembly to explain the decision.

3.2.3.3 Technical

The Board validates the outputs of the Committees, in particular:

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

- the software and consultancy services proposed and provided by the Product and Asset Committee;
- the certification scheme and the certification criteria proposed by the Certification Committee;
- the contracts and pricing proposed by the Profit and Loss Committee.

In case of refusal of validation, the Board informs the Committee for Safeguarding Impartiality and the Financial Committee.

3.2.4 Decision taking

Nominations of Committee members: Simple majority after communication of candidates to all members.

Other decisions: a majority of the members of the Board, e.g., approval by 4 members

3.2.5 Performance

3.2.5.1 Commercial

Monthly monitoring

Appointment of contracts with Secretary, managers, or external experts.

3.2.5.2 Governmental

Board meetings occur:

- at least twice per year or;
- at the written request or the President or Vice-President given at least 24 hours prior to the Board meeting.

3.2.5.3 Technical

Daily incident handling.

3.3Governance applicable to all Committees

3.3.1 Responsibilities

Each committee has specific responsibilities.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.3.2 Members

Each committee is headed by a President – typically a person very familiar with the topic and in his absence by a Vice-President. He reports to the general assembly if foreseen in the governance rules and to the board.

The committee nominates a secretary who convenes meetings, provides reports to members and other committees or boards.

Members are representatives of the BO members, i.e., they shall be proposed or supported in writing by a legal entity that is members of the BO.

Additional to members, experts who do not represent a member can be appointed to assist the work of the committee.

Members are not paid for their work; experts can be paid based on a previous agreement with the Board.

3.3.3 Activities

3.3.4 Decision taking

- Ideally decisions are taken unanimously.
- If this is not possible, decisions are taken after deliberation (via a meeting or email). The president formulates the decision, sends it to Committee members and collects the votes of each member. He/she can fix a deadline (not shorter than 3 days) during which an unsubmitted vote is considered an abstain. The President then presents the result to all Committee members.
- In case of strong dissent, a Committee member can address a formal request to the Board for revising a decision. In that case, the decision of the Committee takes effect only one month later, after confirmation by the Board. This does not apply to the Committee for Safeguarding Impartiality, nor to the Financial Committee.
- Otherwise, the decision can take effect one week later and be announced at that point of time. In case of emergency (e.g., to stop fraudulent and risky activities, the board can reduce this and make a decision applicable immediately.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.4 Committee for Safeguarding Impartiality (CSI)

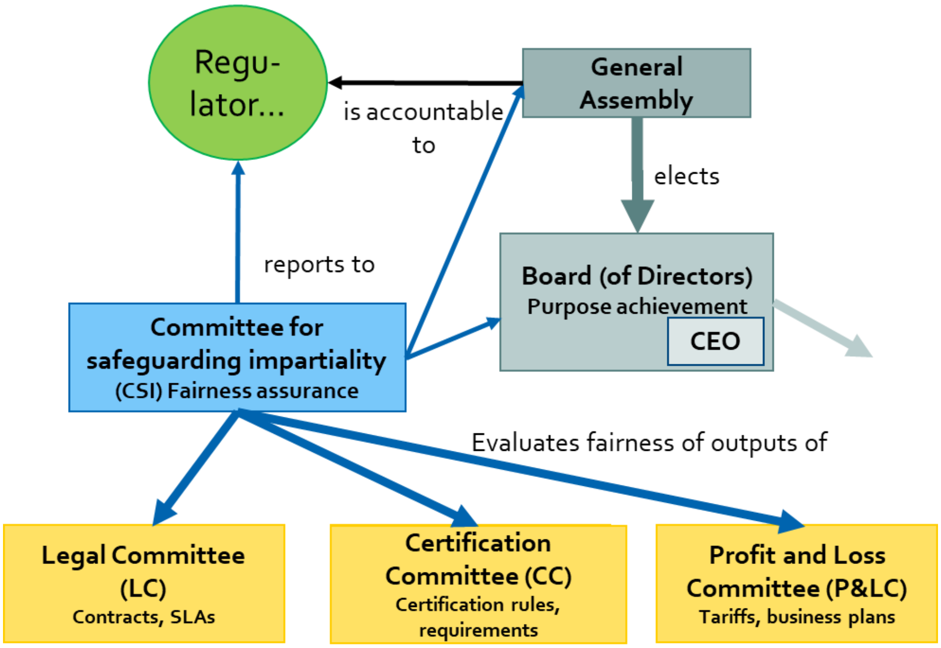

Figure 2: Activities of the Committee for Safeguarding Impartiality (CSI)

3.4.1 Responsibilities

The Committee for Safeguarding Impartiality is responsible to:

a. assure
   - the fairness of contracts with respect to all involved stakeholders,
   - the fairness of the certification procedure and certification criteria (if applicable) for all type of members;

b. communicate
   - an opinion in case of significant changes to internal regulations, internal procedures, certification procedures, certification criteria, to the author and to the decision makers,
   - an opinion regarding complains and appeals to the author and to the addressee,
   - decisions regarding fairness of contracts to the Board,
   - issues regarding fairness to the general assembly;

c. direct nothing;

d. evaluate
   - the mutual interest of involved stakeholders in contracts,

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

- ◇ risk related to the certification procedure;

e. monitor changes of the internal regulations, internal procedures, certification procedures, certification criteria, complains and appeals.

3.4.2 Members

They are nominated by the Board and formally approved by the General Assembly.

They hold their position for two years. The mandates can be renewed or extended by the General Assembly. The General Assembly should not change more than half of the members at once to ensure continuity.

They shall not be members of the Board and shall not be a member of the Committee for Financial Control.

The President shall have proven experience in the field of the relevant regulations.

3.4.3 Activities

The Committee for Safeguarding Impartiality reviews and comments contract drafts to assure that no party is in a disproportionate position of power in the planned contractual agreement. It also reviews the contents of the Certification scheme prepared by the Certification Committee to verify that the scheme's stringency is commensurate (if applicable).

The Committee investigates misbehavior of members or committees.

The Committee shall review output of the other Committees submitted to the Board and that the Board will not have validated. The Committee may in turn consult the General Assembly.

3.4.4 Decision taking

Cf. 3.3.4

3.4.5 Performance

- Frequency of assembly: The Committee for Safeguarding Impartiality will be assembled only when necessary, that is for changes in the main contractual agreement or certification process, to monitor certification bodies and to provide opinion on complains and appeals.
- Deliverables: A report to the Board and relevant Committees detailing the review of the contract contents and certification scheme contents, possibly accompanied by recommendations.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.5Committee for Financial Control (CFC)

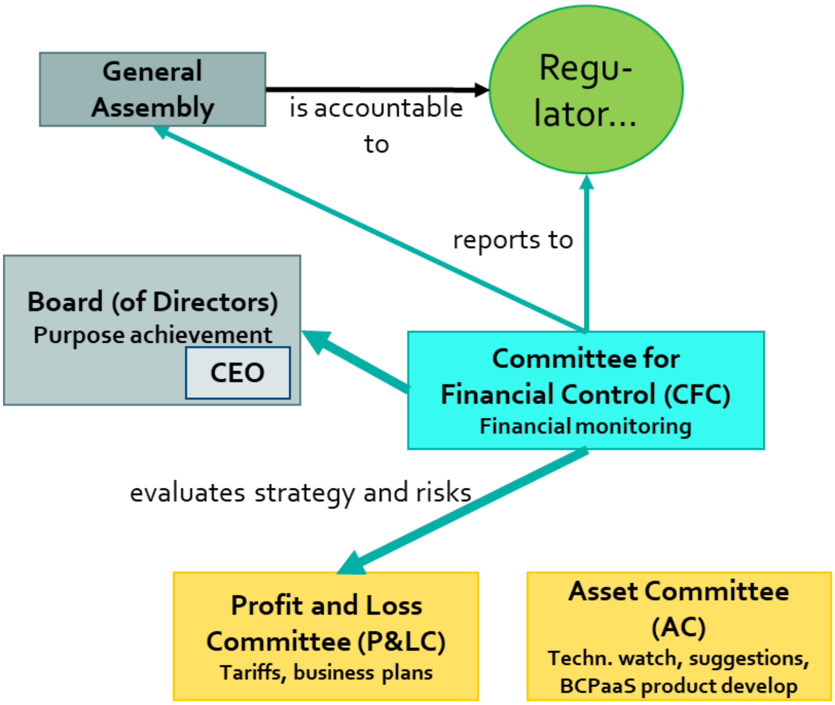

Figure 3: Activities of the Committee for Financial Control (CFC)

3.5.1 Responsibilities

The Committee for Financial Control is responsible to:

a. assure
   - accurate documenting and reporting of the state of the BO transactions and overall financial situation;

b. communicate
   - to the General Assembly and the Board the state of the BO finances and any detected discrepancies;

c. direct
   - nothing;

d. evaluate
   - The state of finances of the BO;

e. monitor
   - nothing.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.5.2 Members

The auditor appointed by the annual general assemble is member ex-officio.

The General Assembly can nominate other members.

Other member car be appointed by the board but have to be validated by the next General Assembly.

Unless otherwise specified in the nomination, they hold their position for 2 years.

They may not be representatives of members who already have representatives in the Board or in the Committee for Safeguarding Impartiality.

At least one member shall be an accounting expert.

3.5.3 Activities

The main activities of this Committee are to:

- review expenditures and revenue for a given period;
- produce for the GA upon request a report on the overall financial situation;
- report any irregularities found;
- report transparently to the General Assembly, independently of the Board;
- recommend to the Board actions to take and corresponding activity changes related to financial aspects.

The Committee shall review output of the other Committees submitted to the Board and that the Board will not have validated. The Committee may in turn consult the General Assembly.

3.5.4 Decision taking

Cf. 3.3.4

3.5.5 Performance

- Frequency of activation: Annually and if needed to fulfil their mission
- Deliverables: one report per activation period to the General Assembly, the Board and relevant financial regulators.

3.6Legal Committee (LC)

3.6.1 Responsibilities

The Legal Committee is responsible to:

a. assure

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

- ◇ BO compliance to relevant laws and regulations, in particular: compliance of the content of contracts and SLAs;

f. communicate
   - ◇ validation and advice on compliance of BO documents;

g. direct
   - ◆ nothing;

h. evaluate
   - ◇ compliance of BO activities to relevant laws and regulations;

i. monitor
   - ◇ upcoming new laws and regulations;.

3.6.2 Members

They are nominated by the Board and formally approved by the General Assembly.

The Committee is headed by a President and a Vice-President.

They hold their position for 2 years.

At least one member shall be a lawyer.

3.6.3 Activities

The legal committee reviews the texts of contracts and SLAs. It reviews relevant laws and regulations in existence and under development. It reviews the high-level specifications and functionalities of proposed Applications prior to their deployment, possibly with assistance from the Product and Asset Committee.

It provides feedback to the board in the form of written opinions.

It prepares the internal regulation and changes, for decision by the board.

3.6.4 Decision taking

See Paragraph 3.3.4.

3.6.5 Performance

- Frequency of assembly: review of relevant legal documents whenever a new regulation or law is in preparation, review of legality when an application is changed
- Deliverables: Report on state of compliance of a given document and suggested edits to that document; report on state of compliance of a proposed application; written opinions on upcoming legislation and/or regulation.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.7 Certification Committee (CC) (If applicable)

Certification is encouraged by the cybersecurity act. The TOKEN project did not plan such certification as not foreseen in the project, but this may be relevant for future commercial service.

That is why such certification activities, should be monitored and if useful prepare in collaboration with certification bodies acting as service provider to reach certification.

3.7.1 Responsibilities

The Certification Committee is responsible to:

a. assure
   - the creation, quality, and up-to-date ness of governance scheme; the compliance of all Committees to the governance scheme and statute;
   - the achievement of required and ideally recommended certification;

j. communicate
   - the description of the certification scheme and any subsequent changes to the GA decisions regarding which entity will actually perform the certification audits;

k. direct nothing;

l. evaluate
   - the governance scheme;
   - chosen auditor;
   - report of certification bodies/auditor regarding conformity;

m. monitor
   - NIS 2.0 directive fostering the use of certification for digital services,
   - activities related to the verification of conformity, e.g. designation of a certification body, approving auditor and evaluators,
   - the process for giving a mandate to a certification body, an auditor and evaluator,
   - auditors' performance,.

3.7.2 Members

Appointed experts shall be normalization experts, security experts, privacy experts, and audit experts.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.7.3 Activities

1. Review of relevant technical and organizational standards in existence or under development. Participating in national and international standardization activities
2. Examine and/or propose certification scheme amendments
3. Take the role as accreditation of certification bodies for the certification scheme.

3.7.4 Decision taking

Same as in Paragraph 3.4.4.

3.7.5 Performance

- Frequency of activation: continuous (processing feedback from HOs on certification)
- Deliverables: Certification scheme and amendments to it.

3.8Profit and Loss Committee (P&LC)

The activity of the P&LC shall be tailored to the exploitation plan (i.e. for TOKEN D6.2).

3.8.1 Responsibilities

The Profit and Loss Committee is responsible to:

a. assure
   - profitable activities of the BO,
   - fair pricing of BO offering to potential customers
   - drafting of contracts and SLAs,
   - pre-sales activities;

a. communicate
   - pricing and pricing rationale to members of the BO and potential customers,
   - revenue forecasts to the board;

b. direct
   - nobody;

c. evaluate
   - effectiveness of pricing, i.e. If pricing is adequate with respect to resources allocated;

d. monitor
   - revenue.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

3.8.2 Members

Appointed experts shall be business analysts for pre-sales activities.

3.8.3 Activities

The Profit and Loss Committee's main activities are to:

- propose membership fees;
- define standard pricing for access to the applications and consultancy services;
- negotiate specific pricing with members;
- establish twice a year a profit and loss forecast;
- update the price tables when needed.

3.8.4 Decision taking

Same as in Paragraph 3.4.4.

3.8.5 Performance

- Frequency of activation: Review of pricing annually; presale activity continuous
- Deliverables: annual report to the Board on the overall offering and justification of any changes.

3.9(Product and) Asset Committee (P&AC)

3.9.1 Responsibilities

The Product and Asset Committee is responsible to:

a. assure
   - the BO's technical product creation, maintenance and quality,
   - the BO's consultancy services,
   - a technological watch over relevant IT fields, with a focus on blockchain in particular,

e. communicate
   - software and all relevant documentation; Advice from its technological watch to GA;

f. direct
   - technical work on BCPaaS software;

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

g. evaluate
    - quality of software;

h. monitor

3.9.2 Members

Appointed experts shall include Designers and developers that create the software used to build up, run and monitor the BCPaaS and IT Security personnel.

3.9.3 Activities

The Product and Asset Committee's main activities consist in:

- patching, maintaining and further developing the BCPaaS,
- ensure interoperability with relevant DLTs,
- providing consultancy services to interested stakeholders,
- implementing a technology watch especially in Blockchain technologies in order to keep the BO offering state-of-the art.

The Product and Asset Committee receives technical feedback from Members. It communicates recommendations for technical changes to the Board for decisions.

The Product and Asset Committee provides the BO's consultancy services, such as:

- acting as a facilitator for a proof-of-concept to help validate its model and suggest improvements to the business process;
- acting as a facilitator for a developed Application to introduce vendors, propose best programming practices and suggest Quality Assurance (QA) rules for the smart contracts, based on operational experience.

It participates in national and international standardization activities.

3.9.4 Decision taking

Same as in Paragraph 3.4.4.

3.9.5 Performance

- Frequency of activation: continuous activity
- Deliverables:
    - software (containers)
    - software documentation for new releases
    - reports on upcoming technologies of interest
    - monitoring of services (i.e., running platform, node hosting…).

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

4 Contractual relationships and data flows

This chapter needs refinement and clarification by the Legal Committee (LC) once the certification schema and the assets have been defined. Questions to be clarified:

1. Financial flows: Provide an idea who must pay whom for what.
4. Common interest: What are the incentives of each actor?

4.1 Overview

Add information later based on T6.2 outcome

Add a dependca garpg (of the differ service provider) for one USEd case a n an illustration

Figure 4: Actors and their contractual relations. the BO interacts directly in relationships with blue arrows (EXAMPLE)

Potential processors for BO should be shown in this diagram, which need to be tailored to BCPaaS or a used case.

4.2 Actors and their roles

4.2.1 The BCPaaS Owner (BO)

The main role of the BO is to oversee the technical development of the BCPaaS and to develop an open sustainable ecosystem around the BCPaaS that will ease the implementation of new Blockchain use cases in the public sector and beyond. It is incentivized to do so by its very purpose, which is to promote and advance the usage of Blockchain technology. The larger and more technologically diverse - in terms of compatible DLTs - the BCPaaS becomes, the greater the success in promoting the overall technology will be.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

4.2.2 Blockchain Application Provider (AP)

A Blockchain Application Provider (AP) is an entity that provides distributed Blockchain Applications that uses the BCPaaS. It is incentivized to do so because the BCPaaS is compliant, interoperable ,xxxx .

An AP is not necessarily a member of the BO.

4.2.3 Blockchain Provider (BP)

A Blockchain Provider (BP) has developed software (or hardware), using blockchain technology, to offer a blockchain service. It has the responsibility that this product (if correctly used) fulfils certain security or functional requirements, which may or may not be tested or checked by independent bodies to a given depth.

4.2.4 Certification Body (CB)

A Certification Body checks whether his customers fulfil given security requirements. Whether these CBs only audit, or continuously monitor and certify, and with regard to which criteria will be discussed in the next chapter. Idem for the question of whether they need accreditation or only a label and/or contractual agreement with the BO.

4.3 Data flow and GDPR roles

To be checked and adapted in the light of Token

PII (Personally Identifiable Information) is transmitted from end users to AP, who legally act as PII controllers.

Structured data (sometimes encrypted or pseudonymized) are distributed to different HOs and, by the very nature of blockchain technology, are no longer under full control of the AP, as the AP cannot decide to delete them.

To protect the data, the APs also rely on a blockchain implementation, i.e., a software including cryptography that is operated by the HO. This blockchain implementation is provided as a license to the AP or the HO by the BO. The BO generally does not access PII; so is not considered as PII processor. However, the security of the provided service, and the need to provide information on vulnerabilities and patches is critical for the protection of PII. That is why this product should have Security and Privacy by design and be approved accordingly.

To ensure security, samples are inspected by Certification Bodies, who act as auditors on the AP, HO, and BP.

In case of AP and HO, the CB has to be considered as PII processor, as in most trustworthy schemes, he has to check on the operational system, and have access to data (not fully, not under full control, but still see and process PII).

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

The BO orchestrates contractual relation between all actors, and may take over some roles, e.g. as a governing entity of the HON, that can stop a HO that is no longer trustworthy and possibly transfer its activity to a different HO.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

4.4 Contracts and business process

4.4.1 Between the BCPaaS Owner (BO) and an Application Provider (AP)

4.4.2 Between an Application Provider (AP) represented by the BCPaaS Owner (BO) and a Host Operator (HO)

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

5 Trust and certification

In this chapter we discuss the different options to ensure certification, which is considered as the basis for trust in the new services and technologies.

5.1 International versus the BCPaaS Owner (BO)-centric

5.1.1 International Accreditation Forum (IAF) Accreditation scheme

The well-known trust scheme of IAF is:

- ISO/IEC 17000, Conformity assessment – Vocabulary and general principles
- ISO/IEC 17011:2017(en), Conformity assessment – Requirements for accreditation bodies accrediting conformity assessment bodies

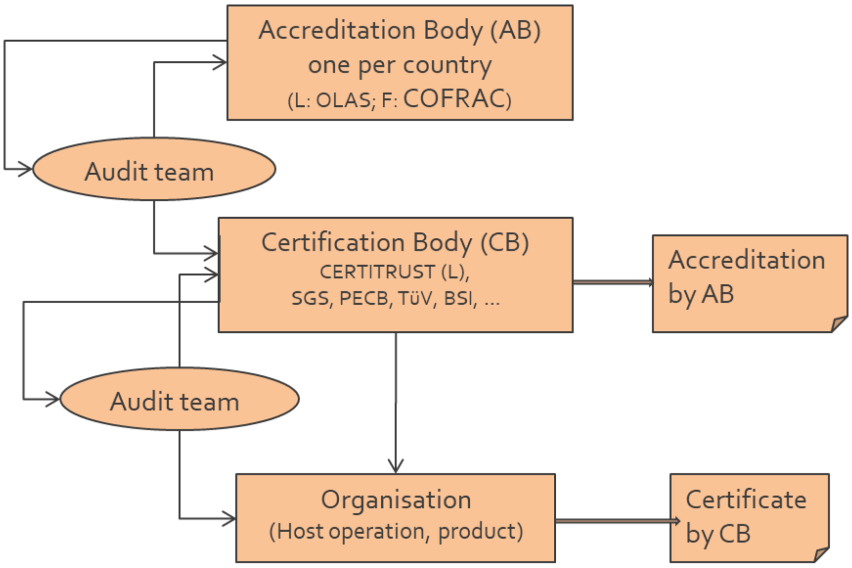

Figure 5: Accreditation scheme

The national Accreditation Body (AB) ensures audit and accreditation of Certification Body (CF) on its territory and provides them with accreditation. As all AB operate under the rules of the International Accreditation Forum (IAF), accreditation assured international recognition of certificates issues by all certification body to which they have given accreditation.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

The Certification Body performs audits and ensures certification of the organization.

The Certification Body shall operate under well-accepted standards:

- ISO/IEC 17021, Conformity assessment – Requirements for bodies providing audit and certification for **management systems**;
- ISO/IEC 17024:2003, Conformity assessment – General requirements for bodies operating certification **of persons**;
- ISO/IEC 17065:2012, Conformity assessment – Requirements for bodies certifying **products, processes and services.**

The Certification body uses different standards as audit and certification criteria when certifying an organization (or a product or a service):

- ISO 9001, Quality management;
- IOS 27001 Information security management system;
- ISO 27701 for privacy management;
- …

It is possible to define, with the BO authorship, a national standard, that defines the BO security requirements, and use this scheme to provide international recognition.

The major drawback of this scheme is that there is currently no experience in applying the new scheme.

That is why we propose to see this as a medium-term objective and start with an internal solution, which is independent of certification bodies and accreditation bodies, but can be easily migrated to a solution using certification body-bearing accreditation for addition trust in the system.

5.1.2 The EU cybersecurity Act certification approach

…

5.1.3 Certification options

1. About accreditation:
   a. the BO assumes the role of the Accreditation body,
   b. OR there is no accreditation at this point.

5. About certification
   a. An audit-and-certification firm assumes the role of the Certification body,
   b. OR a Working group of the BO assumes this role (and delegates the audit activities, not the certificate issuing, to audit companies).

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

Note that we shall distinguish between product and service certification and management system certification, which will be explained in the next section. It is possible to use a different certification scheme for each area.

5.1.4 Proposal

The Committee for Safeguarding Impartiality assures at startup the role of accreditation body, but without following a specific procedure (such as ISO 17065 or Cybersecurity act as it is currently not yet implemented).

As a legal entity, following the certification contract, the BO can be authorized to establish the contract between the certification bodies, and the organization to be certified. the BO does not decide itself on the certification, but only checks the quality and reviews the work of the CB.

When useful to foster trust and international recognition, the board may request CB be certified by a national accreditation body at a later step.

Certification will be paid for directly by the organization to be certified to the certification body. Pricing depends on quantity of work and should be monitored by the Board. The Certification Committee should check that these costs are in line with the revenue of each actor.

5.2Certification of management system versus product, processes, or service

Following definitions of ISO, we distinguish two areas:

- **Certification of a management system**, such as the environmental management system, quality management system or information security management system of an organization, is one means of providing assurance that the organization has implemented a system for the management of the relevant aspects of its activities, products and services, in line with the organization's policy and the requirements of the respective international management system standard.
- **Certification of products, processes or services** is a means of providing assurance that they comply with specified requirements in standards and other normative documents. Some product, process or service certification schemes may include initial testing or inspection and assessment of its suppliers' quality management systems, followed by surveillance that considers the quality management system and the testing or inspection of samples from the production and the open market. Other schemes rely on initial testing and surveillance testing, while still others comprise type testing only.

Both approaches have a lot of similarities, and we propose to start by defining certification criteria:

- according to management systems, as an add-on to ISO 27001 for the Host Operators;

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

- according to products, processes or service for an Infrastructure provider.

5.3Certification criteria

In this section, we discuss actors and their need for certification. Details shall be in separate documents to be established by the Certification Committee.

5.3.1 Certification criteria for a Blockchain (Host Operator (HO)) (product)

This is a product certification for the container as it is deployed on the premises of the HO. This certification should ensure that the Host itself is technically deployed following high standards.

HOs that already have a product certification for container deployment on other Hosts within the BO should be able to go through a 'fast-track' process that allows them to get the BO product certification faster than a HO that has no such certification already.

A dedicated test and certification requirements document, ideally with different levels, should be elaborated. The current guidance is not yet appropriate as it mostly focuses on the operation, see below).

5.3.2 Certification criteria for Host Operators (HOs) (management system)

This is management system certification for the information system within which the Host is deployed. This information system is itself within the HO. The certification should ensure that the Host is deployed within a management system that is conform to high standards of information security management in order to prevent abuse.

A short document of a few additional requirements and a list of mandatory ISO 27001 controls should be elaborated, similarly (but shorter than the technical regulation of Digitization and Archiving).

HOs that already have a certified management system in place (e.g. ISO 27001 or equivalent) should be able to go through a 'fast-track' process that allows them to get the BO management certification faster than a HO that has no such certification already. The process will allow to check the certification documents, check whether all mandatory controls are in the Statement of applicability, check whether the Blockchain activity is explicit in the scope of the ISO 27001 certification, and perform a dedicated audit on the additional the BO requirement (typically one day). This work could be done either by the ISO 27001-CB, or by an entity member of the BO approved by the Certification Committee.

The current guidance is a good starting point but should be structured according to ISO 27009 for better use by external Certification bodies.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603

5.3.3 Certification criteria for Application Providers (APs)

This is a product certification to be delivery according to ISO 27065 (or in future the EU Cybersecurity Act), based on certification criteria to be established by the BO.

As this needs some preparation, it should be considered as a medium-term objective.

5.3.4 Certification criteria for the Orchestration of Host Operators (HOs)

As the BO proposes to define certification itself for its activities, it makes sense that the BO itself should be certified ISO 27001-compliant and GDPR-compliant. However, as this requires preparation, it should be considered a medium-term objective, after startup. In particular, the BO shall already have some operational activity with a first customer and targets for international recognition.

5.3.5 Requirements for the Certification Auditor (CA)

The external auditor performing the HO audit should be a well-recognized actor on the market for information security and should be independent of the target of certification.

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No 870603