Token

Transformative impact of disruptive technologies
in public services

www.token-project.eu

TOKEN Governance Model Analysis

Project full title
Transformative impact of disruptive technologies in public services step

Contract No.
870603

Strategic Objective
SC6-TRANSFORMATIONS-2019

Project Document Number
SC6-TRANSFORMATIONS-2019-870603-WP6-D6.3

Project Document Date
21.12.2022

Deliverable Type and Security
R - CO

Author
LIST (Uwe Roth)

Contribution
Infrachain (Adnan Imeri), LIST (Thierry Grandjean)

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

Contents

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

Introduction

This document provides the result of the analysis and review of the following documents that are related to the deliverable D6.3, that supports the development of a TOKEN Governance Model.

- STA_R630_token-GovernanceReport_v0.2.1-cha.docx (29.9.2022)
- STA_R637_token-GovernanceReviewTempl_v1.2.docx (24.10.2022)
- STA_R638_token-GDPR-ReviewTempl_v1.1.docx (24.10.2022)
- STA_R638_token-NIS-evaluation-ReviewTempl_v1.0.docx (24.10.2022)

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

1 The TOKEN Governance Model

Tasks Description

The project task description of the Governance Model is as follows:

> *The aim [..] is to define the rules that will guide the evolution and maintenance of the TOKEN BCPaaS beyond the project. This includes the definition of the legal vehicle that should handle the ownership of the TOKEN BCPaaS beyond the project.*
>
> *[..] we envision that a TOKEN Association will be established as the body that will handle the operations beyond the project. This will be an independent NGO to support the community and network activities of the project.*
>
> *To enable this activity a bylaw will be created establishing the founding members and the rights and obligations of the different types of membership as well as the rules to decide on the technical evolution of the technological stack that will work as a DAO (Decentralized Autonomous Organization). These members will be public organizations and public service operators, who will deploy Validator Nodes or Regular Nodes within the TOKEN BCPaaS. Other routes for shaping a formal body that will take care of the TOKEN BCPaaS beyond the project, like joining an existing body or establishing a MoU, will also be explored during the execution of this task.*
>
> *The implementation of this task will lead to the definition of the TOKEN Governance Model [: Definition of the legal vehicle to evolve and maintain the BCPaaS].*

Options for Governance

In the description, the intention was to provide a Blockchain Platform as a Service (BCPaaS). The general understanding of BCPaaSs is to provide platforms that allow users to have a simplified process to deploy blockchain applications with the support of a

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

platform. In contrast to that, the TOKEN project developed a set of relevant services for users that benefit from an underlying blockchain but shield any blockchain specific details from the user. This is important, because the TOKEN services are designed to be blockchain agnostic, meaning that the underlying blockchain can be replaced without having an impact on the usage of the service. Users of the services are in fact totally unaware of any implementation details and also do not know if a blockchain is used to provide the service or not. Some of the services in reality do not use a blockchain, e.g., services to store data in the Interplanetary File System (IPFS).

Because of the previously said, a stronger focus was made on the design of the PUCs which use some of the services. Partially these PUC themselves used their own blockchain including the deployment of smart contracts.

With that in mind, governance of the results of the TOKEN project – in contrast to the initial task description – can now be understood in several ways:

(1) Governance of the TOKEN services (as initially foreseen in the project description)
(2) Governance of the TOKEN codebase
    a) as closed source
    b) as open source
(3) Governance of the PUC that make use of TOKEN
    a) by using the TOKEN open-source codebase to run the TOKEN services by themselves
    b) by using the TOKEN services as a third-party service

From discussions in the project, there is a tendency to not govern the token services (1) but to **publish the TOKEN codebase as open source**, as long as it does not affect protected intellectual property of partners (2b). This puts a stronger focus on the potential governance of the PUCs that use the codebase to run the TOKEN services by themselves (3a).

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

2 Deliverables

The deliverable of this task consists of one main deliverable document plus three supporting documents:

- **The Governance Model Report**
  This document provides the key principles and guidance related to the governance scheme, and the prerequisites for a community driven Blockchain Platform as a Service (BCPaaS) with a view towards integrating it to any Blockchain environment.
- **Review template for Distributed Ledger Technology governance (DLT)**
  This document provides guidance to be compliant with ISO/TS 23635:2022 on Blockchain and Distributed Ledger Technologies.
- **Review template for Data protection (GDPR)**
  This document provides guidance to be compliant with the General Data Protection Regulation of the EU (GDPR)
- **Review template for Data protection (NIS)**
  This document provides guidance to be compliant with the Network and Information Security Directive of the EU (NIS Directive)

The Governance Model Report

General remarks

This document provides all relevant aspects to set up an organisational structure that is able to govern the results from the project. The document puts a special focus on open source **but does not detail the specifics to set up an open-source development framework, potentially including supporting community**. From the reading the document describes more the setup of an organisational structure that manages the services of TOKEN as a business. If the document targets both, the provision the TOKEN services (1) and the management of the codebase (2), the structure potentially needs to be doubled in parts, one for the governance of the service, one for the governance of the open-source code-base because the parties that are involved in both aspects are not necessary the same. In case only the governance of the TOKEN services is described, the entire open-source aspect that is discussed in the document might be unnecessary

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

because there is no difference in the governance of the codebase as closed source by the consortium or to publish it occasionally to the public.

Currently the code is developed inside the project. Even if it is managed as open source, it will likely be controlled at the beginning by the project partners who developed the code. How the intellectual property of the platform code is managed after the end of the project should be described in the consortium agreement.

CERTH has already used code in the project that is their own intellectual property, and which cannot be published as open source, but the licence model of any other published open-source code must be decided. It shall be decided if third parties will be free to exploit them as proprietary solutions or not. Components shall be exploited according to their licence. In case of a non-free licence, it shall be made available at fair/favourable conditions, i.e., not locking further exploitation given the fact that such components have been implemented by means of public money.

TOKEN does not necessarily build on a permissioned blockchain. It is said to be Blockchain agnostic, and it could also use Ethereum. This has an impact on the potential need to manage a blockchain infrastructure, potentially managed by a consortium or not. In case TOKEN uses in the backend a public blockchain or uses a consortium blockchain that is managed by a third party (e.g., EBSI), there is no need to create a consortium by a potential TOKEN organisation. Even with a permissioned blockchain, TOKEN adds an interface in front to the used blockchain. Whoever manages that API is the central authority and there might be no need for a consortium in the backend. **The document should reflect this, e.g., in the chapters about contractual relationships or the setup of boards.**

Governance principles

The documents list some governance principles specifically for an open-source system based on DLT/blockchain. With the above said about the blockchain that acts only in the backend, they might not be needed or relevant in a future governance model.

Principle 1: Define identifiers of entities involved

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.

Principle 2: Enable decentralized decision-making

There is no decentralized decision making in the TOKEN services. Services like stamping, storing, and messaging do not require a decentralized decision. Decisions about the

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

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.

Principle 3: Ensure explicit accountability

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.

Principle 4: Support transparency and openness

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.

Principle 5: Align incentive mechanisms with system objectives

The link between incentives and SDG is not obvious and feels a little out of the place. Since the TOKEN services are blockchain agnostic, it is not clear how incentives of the blockchain support the objectives of the TOKEN platform.

Principle 6: Provide performance and scalability

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.

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

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.

Principle 8: Ensure security and privacy

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 foresee creating a certified product for which a certification needs to be maintained if changes are applied or if new risks appear. That's why the customer should follow an ISO 27001 approach when managing the operation of a process with

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

SW testing, system security monitoring, etc. Review templates for GDPR, 27701, and 27002:2022 have been prepared by TOKEN.

Principle 9: Consider interoperability requirements

It is said that the TOKEN services are blockchain agnostic. In that case, 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.

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.

The governance of an open-source system

All relevant aspects to set up an organisational structure with its elements of a governance of an open-source system are explained. As already explained earlier, the focus is on an open-source system and less on a TOKEN service provider. The structure might need refinement based on the route that will be taken. In parts it seems there are more elements than are actually needed.

Technical aspect and assets

Such a section would help if it was put on the front of all chapters. This way it would be clear on the options on what is governed (source code or service) and details about that.

This section also mentions the other use cases. It is not clear how an explanation of other use cases helps in this document.

Contractual relationships and data flows

This section is focusing too much on blockchain related actors and their roles.

Trust and Certification

This section should benefit if the actors like Business Owner, Host Operator, Application Provider, Infrastructure Provider could be linked to the entities of organisational structure or if their relation is clarified. The same for the relation between Certification Committee and the Certification Body, which is not entirely clear. In fact the entire section describes elements that are quite generic and would fit every newly created organisation. A simplification based on the likely outcome of the project would help.

The Review Templates

The review templates consist of templates about the Distributed Ledger Technology governance (DLT) and Data protection (GDPR, NIS).

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

The Governance template (DLT) builds on an ISO standard. The template can only be used for evaluation if the standard was bought.

From the description, the TOKEN services are Blockchain agnostic and therefore could build on a public blockchain like Ethereum. In that case, governance of the blockchain network is not an issue and it is not in control of the project. The template seems to cover only the case of a permissioned consortium blockchain that is in control of TOKEN.

This document only covers DLT related aspects, but TOKEN also includes IPFS. Additionally, PUCs also use DLT (some even two: Fabric; Indy) plus one or several local databases, or wallets, or policy/role/identity management systems. After reviewing all templates, it seems that even the GDPR and NIS template are not fully covered, since they only cover GDPR aspects. Potentially there are other ISO standards that could be applied.

On the other hand, the GDPR and NIS templates seem to cover many more aspects than are relevant in the project. The nature of the services that are provided by TOKEN, e.g., stamping, do not even apply to data protection as no personal data is processed. A critical view on all these requirements in the light of the TOKEN platform would help to simplify the evaluation process.

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

3 Conclusion

The use of dedicated TOKEN services in the PUCs are only minimal:

TOKEN Service and Component		Type	PUC 1 Public Funding Distribution	PUC 2 Transparent Management of Public Accounts		PUC 3 Last Mile Logistics	PUC 4 Data Valorisation Service	Σ
				Procurement	e-Voting			
Notarization	Stamp API	Service	●					1
	Anchoring API	Service	●					1
	Canis Major	Compo-nent				●	●	2
Decentralized Identity	~~Token Connect~~	Service						0
	CERTH SSI	Compo-nent		●				1
Messaging and Events Streams	Token Streams API	Service	●					1
Distributed Storage	~~IPFS Web Gateway~~	Service						0
	IPFS Storage & Pinning Service	Service	●					1
	~~IPFS Private Datastores~~	Service						0
Σ			4	1		1	1	

- Only PUC 2/CERTH use the CERTH SSI component:
  CERTH will maintain the CERTH SSI component as closed source with their own governance/business model.
- PUC 3 and PUC 4 use the Fiware Canis Major component only and no other TOKEN component or service:
  Fiware will maintain the Canis Major component as open source, with their own governance/business model.
- Only PUC 1/FundingBox use the TOKEN Stamping/Anchoring/Streaming/Storing services. No other PUC does.
  It is likely that fundingBox will maintain the

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

Stamping/Anchoring/Streaming/Storing services as part of the PUC1 development or use them in new projects. The code of these services will be published as open-source.

Summary of the governance of the TOKEN components/services:

- CERTH takes care of business/governance of CERTH SSI.
- Fiware takes care of governance/business of Canjis Major.
- FundingBox takes care of governance of Stamping/Anchoring/Streaming/Storing services, but not as a TOKEN platform and without a business in mind.

Summary of the governance of the PUC:

- PUC 1/3 will exploit their results in new projects.
    - It seems that there are no plans to setup and manage consortium blockchains for these PUCs.
- PUC 2/4 will try commercialization.
    - PUC 2 uses a blockchain to manage business logic plus Hyperledger Indy as part of their CERTH SSI component. It does not seem that they plan to setup and manage the blockchain as a consortium blockchain.
    - PUC 4 uses the Alastira Blockchain behind Canis Major. Alastira Blockchain is a public/permissioned blockchain, not managed by the PUC owners. The PUC owners do not manage the consortium behind Alastria, they are only users/consumers of that service.

It seems to be consensus that the results of the TOKEN platform will only be published as open source. There will be no organisational structure that takes over the running and maintenance of the TOKEN service, and there will also be no consortium and community creation that manages and improves the code base. This makes the governance model document and the supporting template documents mostly obsolete. On the other hand, the PUCs have a higher chance to continue after the end of the project. A revision of the governance model document and the supporting template documents away from the focus on an open-source BCPaaS system, but more to support the governance of the PUC would be a way to maintain the valuable information of these documents.

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

4 Suggestion

It is suggested to see all the work that has been done so far (main document plus supporting documents) as a source of modules and building blocks, without making assumptions on blockchain consortia, open-source consortia, or other types of structures. By checking the business plans of each PUC developer or TOKEN service/component developer, it must be decided on which of the modules and building blocks are relevant for that specific case. From the overview table of the use of the various use cases and answers from a questionnaire, the following can be concluded:

- The CERTH SSI component:
  - CERTH takes care of business/governance of CERTH SSI.
  - CERTH will maintain the CERTH SSI component as closed source.
  - CERTH uses their own governance/business model.
- The Fiware Canis Major components:
  - Fiware takes care of governance/business of Canjis Major.
  - Fiware will maintain the Canis Major component as open source.
  - Fiware uses their own governance/business model.
  - There is no plan for commercialisation of the results.
- The TOKEN Stamping/Anchoring/Streaming/Storing services.
  - FundingBox takes care of the governance of Stamping/Anchoring/Streaming/Storing services.
  - The code of these services will be published independently as open-source, not as part of a TOKEN platform
  - There is no plan for commercialisation of the results.
  - FundingBox will maintain the Stamping/Anchoring/Streaming/Storing services as part of the PUC 1 development or use them in new projects.

The PUC owners described the governance of their PUC as follows:

- PUC 1/3
  - There is no plan for commercialisation of the results.
  - They plan to exploit their results in new projects.
  - In both PUCs there are no plans to setup and manage consortium blockchains.

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

- PUC 2
    - There are plans for commercialization of the results.
    - PUC 2 uses a blockchain to manage the business logic in the form of smart contracts, plus Hyperledger Indy as part of their CERTH SSI component.
    - There are no plans to setup and manage the blockchain as a consortium blockchain.
- PUC 4
    - There are plans for commercialization of the results.
    - PUC 4 uses the Alastira Blockchain behind Canis Major.
    - Alastira Blockchain is a public/permissioned blockchain, not managed by the PUC owners.
    - The PUC owners do not manage the consortium behind Alastria, they are only users/consumers of that service.

With this, the governance of the commercialization of the PUCs 2 and 4 remain as well as FundingBox' plan to publish the Stamping/Anchoring/Streaming/Storing services as open source.

For each of the three cases it should then be decided:

1) Which modules or building blocks of the Governance Model are specifically needed to setup a legal organisational framework?
2) Which paragraphs of the GDPR and NIS laws must be considered?
3) Which tests of the ISO/TS 23635:2022 standard must be executed?

This would be useful because not all models, laws and tests are relevant in all cases. It would help to know only the relevant, depending on the case of governance.

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