→ A DISTRIBUTED LEDGER APPROACH TO MODEL BASED SYSTEM ENGINEERING

Executive Summary

ESA Contract No. 4000135358/21/NL/GLC/ov

Redouane Boumghar (Parametry.ai)
Annalisa Riccardi (University of Strathclyde)
Ashwin Arulelvan (University of Strathclyde)
Edmondo Minisci (University of Strathclyde)

European Space Agency
European Space Research and Technology Centre
Keplerlaan 1, 2201 AZ Noordwijk

October, 2022

1 EXECUTIVE SUMMARY

In the last 10 years, Distributed Ledger Technologies (DLT), of which blockchain is a particular kind, have initiated a paradigm shift in data and value transactions, by removing a central authority and propose a decentralised and distributed system ruled by semi automatic procedures to validate and authorise transactions.

DLT has gained a lot of attention from both academia and industry. Apart from the financial sector, they have been applied to variety of domains such as healthcare, IOT, energy, supply chain, to provide a solution for sharing and tracking of domain specific data and information with an immutable history record for each transaction.

Currently the application to DLT in Model Based System Engineering is largely unexplored. To our best knowledge, there is no published work to date that have explored the possibility of applying DLT to concurrent design and system engineering lifecycle.

The ***Objectives of this activity*** are:

- Assess the applicability of distributed ledger technologies for inter and intra Agency system model's data sharing and tracking.
- Develop an integrated prototype to evaluate and assess data accessibility, management and tracking from multiple peers in a decentralized network.
- Assess how the overall system is able to track ownership, reach consensus, operate without a central authority and prevent any unauthorized exploitation of data (privacy & security).
- Assess how such system is able to advance on current MBSE challenges, namely control and tracking of system model data exchange across the different system design phases.

When a highly centralised process is decentralised and the central authority is removed, what is created effectively is a Decentralized Autonomous Organization (DAO). The DAO serves to represent the contracts between all stakeholders, when they can be called and how they can be automated at their most (contracts calling other contracts). These contracts are called smart contracts in the blockchain and they encode the business logic of the MBSE processes that we have modelled.

Two use cases have been investigated and developed to demonstrate the applicability of DLT to MBSE.

The first use case is called ***Engineering Identities***. At ESA, internally, system engineers are identified on the system. Contracting companies might have different engineers working on the same project non-simultaneously. A decentralized identification system could help provide LSIs and contractors with the possibility to generate sub-identifications for their personnel allowing to keep a great granularity of information on the audit trail, and enabling to reach feedback from the right person at the right time. In this context system engineers are considered *provers* of their identity thanks to the system. Companies or ESA are *issuers* of digital identities while different participants providing services on the network, are *verifiers* of identities. The paradigm shift driven by the decentralisation is twofold. Firstly, the deliverance of access authorization becomes decentralized, instead of delivering accesses, ESA would have to deliver certificate issuer rights to companies contracted to work on co-design projects. ESA would therefore delegate the issuance of certificates. Secondly, Engineers are directly identified as their affiliations, meaning that even if they change companies,

it is still possible to trace changes made by one person over one or several projects. While this first use case is limited in showcasing the advantages in of a decentralisation of the MBSE process, it is a necessary step to be developed to have multiple authorised entities interacting on the blockchain.

The second use case is called ***Digital engineering models and zero-knowledge proof scenario***. Digital representation serves to replicate real asset behaviour in simulated environment using external or internal data streams or information. Digital smart assets representation on the blockchain offers a way to verify the authenticity of states from owned twins but also from externally owned twins, without knowing their exact specifications. Moreover in specific missions, some components of the space mission might require special access rights to their models, their performances criteria or other sensitive variables. Such information might be protected by commercial secrecy or a need-to-know to confidential defense status (or higher) for the person or system trying to access it. Protecting sensitive information is what privacy solves, whereas ZKP provides a probabilistic solution to demonstrate that one party knows the sensitive information without revealing that information, neither offering possibilities for inference of that information. We demonstrate the integration of zero knowledge proofs and the digital representation of the physical assets within the developed blockchain system. Digital assets are modelled with non-fungible tokens (NFTs) smart contracts. These have the advantages that they can represents uniquely an asset, also across different projects, with the flexibility of adapting their metadata information. ZKP are demonstrated on a mass margins verification problem. The mass of a component is verified to be within a known range of values without the need to reveal its exact value that can remain private information of the supplier.

The activity has successfully developed and demonstrated the first prototype of a distributed and decentralised MBSE system that acts as a global configuration tool for project and assets managements of space mission design studies. It helps progressing the development of solutions that can address the MBSE challenges of controlling data exchange and traceability across system development and operations lifecycle. This is achieved in this project through the introduction of digital engineering identities and digital representation of physical assets, that provides a trustable and immutable single source of truth of shared information. Moreover the project demonstrates how a DLT system can embed the necessary business logic and protocols to automate the verification of information when only partial knowledge is available. This is done with the integration of ZKP protocols within the blockchain.