DECENTRALIZED TRUST MANAGEMENT IN CONCURRENT DESIGN USING BLOCKCHAIN

Redouane Boumghar[1] ⊕, Shahzad Ameen[1], Prof. Dr. Annalisa Riccardi[2],
Prof. Dr. Ashwin Arulselvan[2], Prof. Dr. Edmondo Minisci[2],
Dr. AnhToan Bui Long[3], José Pizarro De La Iglesia [3]

[1]***Parametry.ai***
Frankfurt am Main, Germany
Email: red@parametry.ai⊕, shahzad@parametry.ai
⊕: corresponding author

[2]***University of Strathclyde***
16 Richmond Street, Glasgow, G1 1XQ, United Kingdom
Emails: annalisa.riccardi@strath.ac.uk, ashwin.arulselvan@strath.ac.uk, edmondo.minisci@strath.ac.uk

[3]***European Space Agency***
ESTEC, Keplerlaan 1, 2201 AZ Noordwijk. Netherlands
Emails: AnhToan.BuiLong@esa.int, Jose.Pizarro@esa.int

October 13, 2022

INTRODUCTION: NEED FOR DECENTRALIZATION

Concurrent engineering enables the creation of complex designs in a very short period of time. It involves a multitude of stakeholders that interact in a distributed manner, moving away from the traditional sequential asynchronous process to an iterative and real-time one. Nevertheless a lot of information stays off the books, and knowledge is only partially captured, making explanations of decisions difficult. The risk of wrongly orienting the design from a partially observed situation is high. Concurrent design compensate these issues thanks to frequent iterations. Mission design considerably reduced in the last years thanks to this.

However current digital solutions for concurrent engineering lack a proper way to augment an ergonomic knowledge capture and to interact with automated services that are starting to emerge, to organize information (ontologies) and to use that information for AI generated designs.

Partial knowledge, including unknown and unverified information, can lead to subjective consensus, where issue resolutions become harder. In centralized mechanism we tend to forget human beings at the center have to compile all gathered information, a consequent large cognitive load. In such situations a compromise can arise between wait time for the whole ecosystem of stake holders and quicker partial verification.

Space institutions involved in concurrent design nevertheless possess impressive catalogs of successful missions, perhaps at the cost of destabilized human factors and an exhausted central authority. If cases arise that system engineers might have been forced, by context, to blindly trust counter parties, then this is sign of potential automation of processes.

The proposed approach here is part of an explorative study (OSIP) aimed at applying distributed ledger technology to model-based system engineering and measure the potential shift of paradigm. In every decentralization and desintermediation effort, the most impacted paradigm is the management of trust.

Blockchain technology is used to augment trust in decentralized decisions. Blockchain offers a digital distributed ledger and a distributed virtual machine. The ledger permits to have a single source of truth and the maintenance of a coherent state across blockchain participants. The virtual machine offers capability to execute scripts (smart contracts) that would maintain transitions in the system state. Smart contracts can be triggered by blockchain events or by manual calls, they can also be called directly from other smart contracts. Thanks to a set of smart contracts, a digital automated

protocol is set to enforce business logics to happen with specific and strict inputs and outputs. It ensures that a clear capture of information becomes part of the business process requirements and execution.

Blockchain of different types are used in many different industries in abstractly very similar ways: verifying and signing claims in a distributed manner.

A study from ETH Zürich [1] sets up a flow diagram (1) to decide whether we need a blockchain and which kind we would need. The flow diagram helps differentiating whether the need goes toward a permissioned blockchain, a blockchain where each participant needs to be authorized to join the decentralized network, in opposition to permissionless blockchains. The diagram also distinguishes the need for public versus private blockchain by judging whether public verifiability is necessary.

Unfortunately this diagram does not take into account the efficiency aspect that a blockchain brings in cases where you know all your stakeholders, here the writers. There are many advantages to use blockchain in the purpose to desintermediate the organization of a project, especially in case where this is synonym of efficiency. Aspects like managing crossed jurisdiction or compliance reporting are also missing from such diagram. Such aspects can become extremely important in large space mission which are built with entities from different sovereign states.

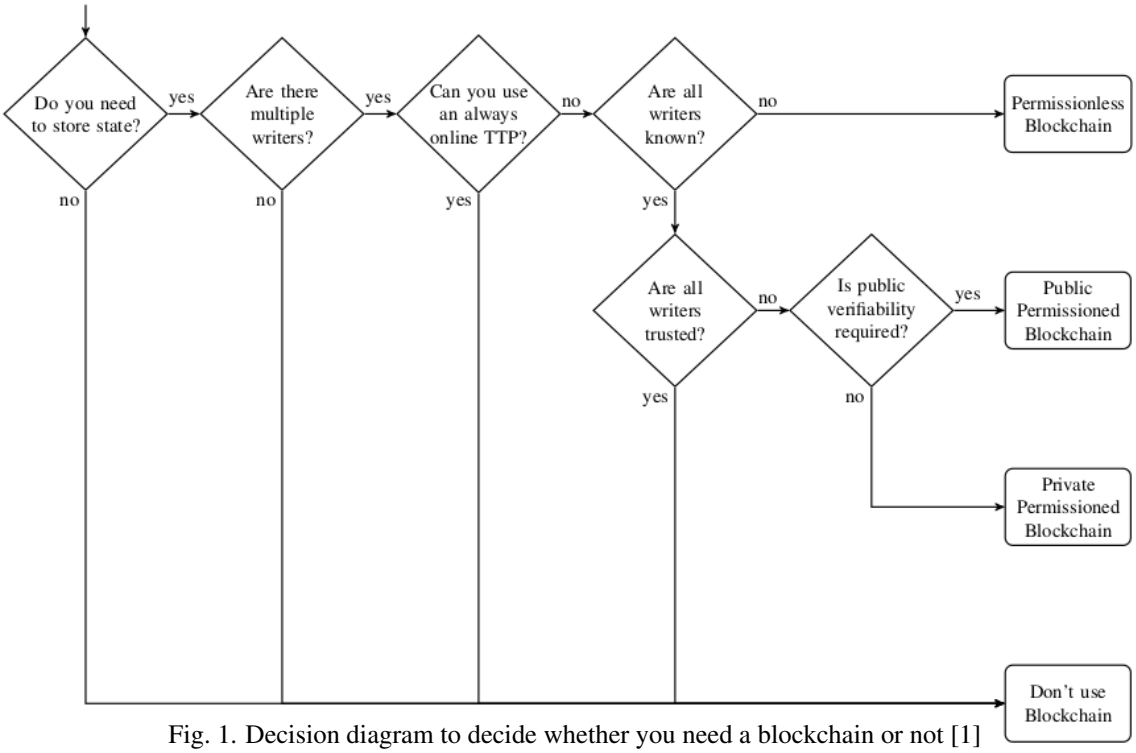

Fig. 1. Decision diagram to decide whether you need a blockchain or not [1]

In summary key points are to be considered to when a blockchain is useful:

- Single source of truth and accountability on state changes
- Wherever consensus is more efficient than centralized decision
- Wherever centralized decision can be automated
- Wherever agility can be or must be improved

EXOCHAIN: DIGITAL IDENTITIES

A private blockchain, named Exochain, is proposed with a proof of stake consensus following the Ethereum protocol. All permitted Exochain participants provide storage and computing resources to the network. Block creators are selected by an election mechanism based on their stake and certain randomness before they can validate all transactions and sign blocks. Contingency processes are present in the Ethereum protocol to replace the elected block creator if this one were to fail. Unlike proof of work consensus, no heavy computation is required.

All stakeholders and entities, participants in concurrent design activities, must be identified on Exochain. Digital identities, represented by smart contracts, are deployed everytime someone wants to start interacting with the network. Before being able to accomplish actions, each digital identity must be claimed by legal entities (ESA, LSIs or any other contractor), thus permitting agencies to let the contractors add any workforce necessary for their work packages. Each personnel holding a digital identity can act on behalf on another entity's digital identity if they have been claimed and allowed to do so.

Digital identities are the source of all actions on our proposed blockchain, controlling permissions to act upon objects in a very granular way without having to deploy a centralized permission management authority. Every action and every actors being recorded in a distributed shared ledger, a detailed audit trail can be made knowing who did what for whom on behalf of what or who. It also enables very fine authorization controls where skills can be required and verified to allow certain actions to be achieved.

Every time contractors and subcontractors interact with the network their trust levels can be adjusted. Actions of participants increase or decrease the trust the network assign to them. It would at the same time decrease, create or reinforce links between skills and their digital identities.

EXOCHAIN: DECENTRALIZED MISSION DESIGN

In order to design a mission, elements needs to be represented on the blockchain. this representation is what is called the tokenization of assets; a smart contract represent an element, its options and various versions/iterations. One of the paradigm shift is that Exochain does not manage mission and element options and iterations (or versions) the same way software such as COMET would do.

Each element has independent options which have their own version control, permitting them to evolve independently from what usage was made of which of their versions. Therefore engineers can work on elements to directly fullfil requirements without impacting the current mission version.

The concept of version in Exochain is therefore a voting mechanism; the work in progress on an element or spacecraft is validated once a set of allowed identities voted on its latest option version. Vote proposals are made by subsystem or system engineers whenever an element is ready for evaluation.

Global configuration is then set by linking all version in usage from all elements included in the mission. Unused elements can still evolve until they are elected to be used. This permits to maintain a catalog of components that could be well reused across missions with their own independent audit trail.

The extended architecture shows an opening of interactions with an external storage and computation capabilities, to request external validations and cover some of the mechanisms of zero-knowledge proof (ZKP). Figure 2 includes an external component in blue (visible as step 2') which can serve different purposes and also be, a plug and play interface for external services; such as spacecraft trajectory computations, the third-party managing authorities services or space awareness services (for warnings against space debris).

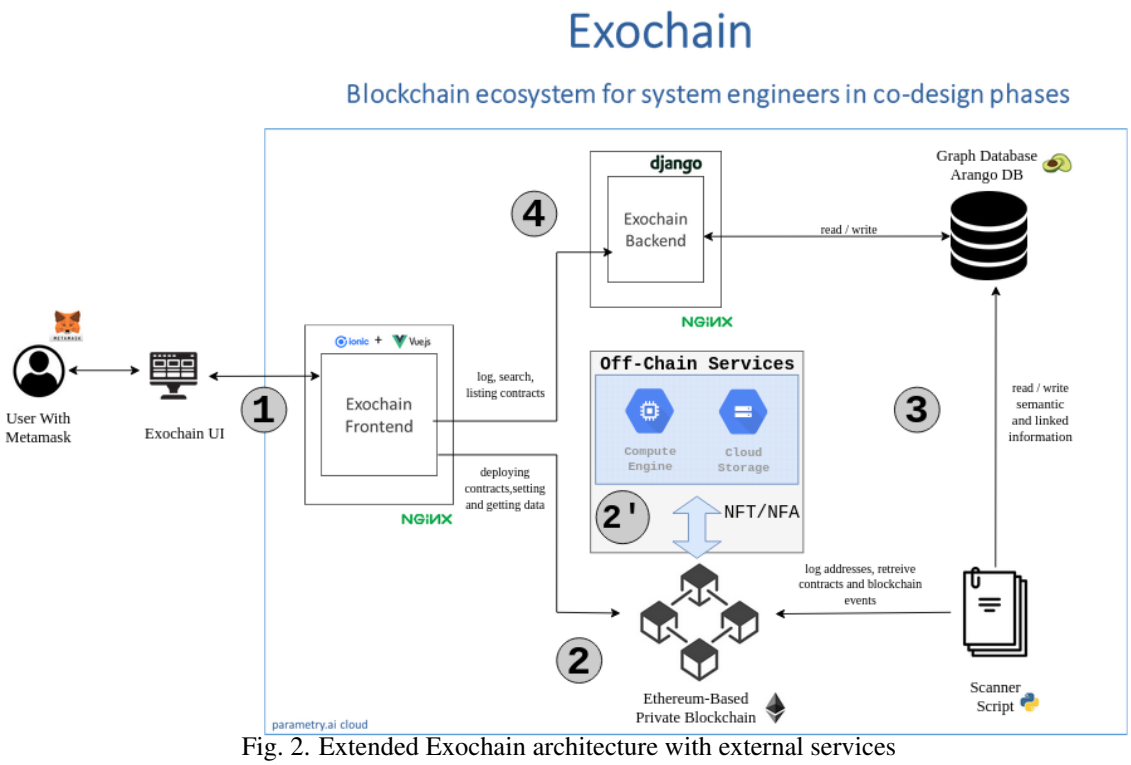

Fig. 2. Extended Exochain architecture with external services

Spacecraft instruments or components are also subject to trust management. Certain components are transparent and their specifications are visible to all system engineers. Other components might have confidential information that must remain undisclosed. These components nevertheless, considered as smart object, need to prove their consistency with the design without revealing their specifications. The Zero Knowledge proof (ZKP) process is used to respond to integration questions without revealing components information. The network issues recommendations on components thanks to participants feedback (in form of votes) or via external optimization services plugged to the blockchain.

CONCLUSION

The impact of a change of trust in a stakeholder, component or overall design can lead to a cascade of consequences:

- Human factors can be destabilized leading to non-constructive team spirit
- Roles and Responsibilities: when a stakeholder trust passes under a given threshold, their roles and responsibilities can be impacted, eventually autonomously triggering parallel autonomous actions (triggering meeting events, finding replacement, holding payment, etc.). This usually takes a lot of time in a traditional project framework. For a component this becomes a go/no-go situation and its selection ranking might be directly impacted.
- Procurement: change of responsibilities might directly impact procurement terms. More or less insurance might also be requested.
- Accountability: with gain in responsibilities comes greater accountability which is rarely adapted in the course of a project.

The experience of decentralization can be brought in an iterative way to engage in a smooth shift of paradigm. The following gradual steps show future potential utilization of such blockchains:

- Managed identities in a decentralized manner;
- Model skills attributes or capacity to fulfill published specifications (for a component) by adding attributes of confidence or expertise levels;
- Propose a governance model to add up skills or attributes to the network;

- Model the stakeholder or engineer participants with respect to available skills, enabling auto-proposed team match-making;
- Allow trust endorsement of a given stakeholder;
- Full mission digital representation on the blockchain;
- Decentralization of mission proposals and automation of procurement.

Blockchain native decentralization is an advantage in the definition of a decentralized trust model and an essential tool in peer endorsement. A decentralized autonomous organization (DAO) for concurrent design creates an important shift of paradigm; the capacity to automate project management and its procurement. Project activities become assessed by the network, acting as judgement platform, and objectivity grows with the decentralization of trust. Hence procurement activities might be automatically triggered by what happens on such blockchain. Moreover, the selection of contractors or components would be replaced by the network of stakeholders choosing who works on what and how in a trustless manner; the network is initialized by a space agency without requiring prior trust on stakeholders. This would set concurrent design to happen as a complete DAO.

REFERENCES

[1] Karl Wüst and Arthur Gervais. "Do you Need a Blockchain?" In: *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. June 2018, pp. 45–54. DOI: 10.1109/CVCBT.2018.00011.