Hyperledger Sawtooth Blockchain for IoT-Blockchain Based Ecosystem

Luc Gerrits, Roland Kromes, Tetouhe Kilimou, François Verdier
Université Côte d'Azur - LEAT - CNRS UMR 7248
Campus SophiaTech Bâtiment Forum Haut,
930 route des Colles, BP 145 06903 Sophia Antipolis cedex, France
firstname.lastname@univ-cotedazur.fr

1. Introduction

Population is becoming aware of the importance of security, traceability, trust and privacy within everyday objects (IoT). Thus these issues are becoming hot topic in research and in industrial developments. The amount of data produced by the IoT is currently stored in a centralized database. Blockchain technology allows decentralized data storage and could allow more secure environment. This intrinsic property of blockchain can provide a solution for the mentioned concerns. Our aim is the integration of blockchain technology within IoT domain. Our project takes part in the Smart IoT for Mobility multidisciplinary project [1].

2. State of the Art

In a survey by Andoni *et al.* [2] a list of 140 companies in 2019 use blockchain with IoT. This shows the interest of integrating blockchain within IoT devices. A numerous of existing blockchain are currently on the market. Lots of them are targeting different application fields (currency exchange, energy grid, supply chain, etc.).

2.1. Blockchain and smart contracts

Since the creation of the Bitcoin cryptocurrency, multiple decentralized systems using blockchain and smart contracts have emerged. Among this trend we witness the increase of usage of IoT (Internet of things) devices. Blockchain provides a distributed record of data with immutability, transparency and a consensus between participating nodes. The consensus allows to have an agreement between nodes. Multiple consensus algorithms are available (Proof-of-Work, Proof-of-Elapsed-Time, Practical-Byzantine-Fault-Tolerance, etc.). IoT devices allows every objects to communicate data and implement an application on the object. Depending on the blockchain technology or setup, it is possible to make it public or private.

Public blockchains have on one hand, the advantage of trust and security. Anyone can and is encouraged to participate actively in network. The risk of an attack or record modification is much more difficult to detect and, because of transparency, the public blockchain must be verified. But on the other hand, public blockchains are known to be slow to reach consensus and lack scalability. Consensus rules are in this case very difficult to verify. Currently new consensus rules are actively being developed to solve these issues.

Private blockchains, also known as consortium blockchain, are blockchains with added permissions to the network. Permission is required to participate actively in the blockchain network. The general purpose of private blockchains it to build a blockchain controlled by one or multiple organization and provide a ledger used to verify and authenticate data origin. Consensus rules enable to creates a system that can be easily managed and updated, delivering a blockchain with a transaction speed much higher then public blockchains. A private blockchain is chosen for our use case structure (Sect.3).

Smart contracts are protocols (commonly known as programs) that are executed on the blockchain. Smart contracts are only available on blockchain that supports them. They are deployed directly on the network and provides the blockchain automation and permits to build applications on top of the network. The smart contracts is the link that can bring IoT and blockchain technologies together. The usage of these smart contracts is described in Sect.3.

2.2. Related works in Blockchain IoT

IoT devices are constrained architectures with well-known hardware limits. These limits are the small memory footprint, the finite battery life, and the low computational power. Blockchain technology requires significant computational power, and its database increases infinitely. Thus, the integration of blockchain technology within the IoT domain is a challenge in the research area and industry. The authors of the most significant related works [3], [4] have combined blockchain and IoT networks. In these implementations the devices do not contain the copy of the blockchain, but they can interface with the nodes of the blockchain using additional application layers.

3. Our implementation and use case

In our blockchain-IoT network, we aim to meet the expectations of a new use case, that was imagined by our industrial car manufacturer partner Renault.

In the imagined use case the vehicle fleet of Renault is connected to a blockchain-based cloud system. In this ecosystem, several entities would be present, as the car manufacturer, an insurance company, the car mechanics and the expertise. The cars' sensors would record the vehicle's environment and the driver's behavior. When an accident occurs, the data recorded by the car would be sent to the InterPlanetary File System (IPFS), which is also based on a distributed ledger technology. The hash of the recorded data is a unique fixed-size representation of this data (often 256 bits or 512 bits). The hash stored on the blockchain is immutable, and it also serves as the reference to the raw data stored in IPFS. In the blockchain, we have implemented a module that allows the write access to the IPFS system only for members (IoT devices) taking part in the ecosystem.

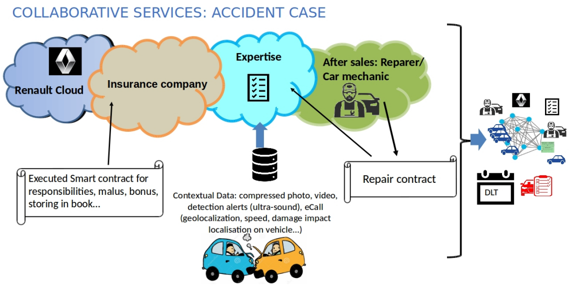

Figure 1: Renault use-case

3.1. Blockchain-IoT Network Architecture Implementation

In our implementation we use the smart contract to identify the IoT device, and actions are executed following the smart contract business logic (e.g. a *new_owner* action declares a new car owner for the ecosystem).

The architecture of our implementation includes a Hyperledger Sawtooth [5] blockchain network (5 nodes) using PoET and PBFT consensus. A custom transaction processor (TP) was designed to accept transactions following the use-case requirements of events and actions. In Hyperledger Sawtooth a TP is similar to a smart contract commonly used in other blockchains. The exception of TP is that it is a module placed on all nodes next the validator.

Data and transactions are generated on a Raspberry Pi 3 B+ model and they are sent to the blockchain network REST API. A custom C++ library was created to build and send transactions to Hyperledger Sawtooth.

As we mentioned in the use case the vehicles contain the IoT devices that are used for sending the measured data to the blockchain. This data would be measured by different types of sensors like radars, lidars, cameras, etc. In our related work [6], the total execution time and the time that is occupied by the hash creation takes up to 34.1% to process 1MB of data. In this work we propose an hardware accelerator module to speed up the hash creation procedure.

Furthermore, our study analyses the performances of Hyperledger Sawtooth blockchain equipped with IPFS module. The PoET and PBFT consensus rules were applied. In Fig.2 we conclude that in a local setup of 5 nodes we can achieve a mean commit rate of 2.7tx/s (i.e. finalized transaction rate).

4. Conclusion

In our study we successfully built an architecture based on IoT and blockchain (Hyperledger Sawtooth) technology. In this implementation the raw data of IoT devices are stored on an IPFS distributed ledger, and the hash of the raw data is sent to the blockchain. An authentication logic

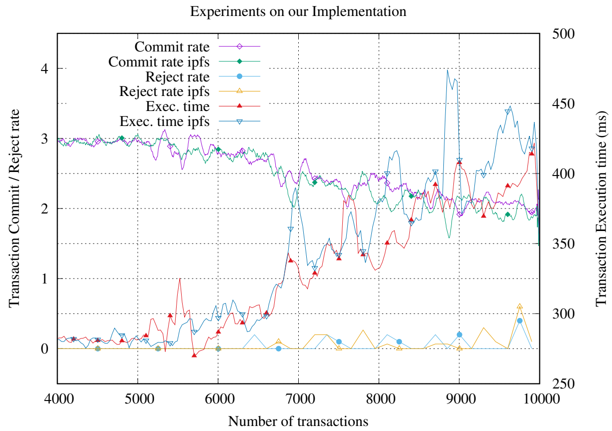

Figure 2: Experimentations on our implementation using PBFT consensus.

was also implemented which allows the data storage on the IPFS system only for identified members of the ecosystem.

In further work, we use specific benchmarks to analyse Hyperledger Sawtooth blockchain implemented in a cloud architecture. The goal is to improve performances and explore the limits of Hyperledger Sawtooth with PBFT consensus using different network and node configurations. The results will determine if this blockchain corresponds to our use-case requirements. French insurance estimates at 55k the total annual car accidents, thus conducting to less than 1 transaction per second [7].

References

[1] F. Verdier *et al.*, “Smart IoT for Mobility: Automating of Mobility Value Chain through the Adoption of Smart Contracts within IoT Platforms,” in *17th Driving Simulation & Virtual Reality Conference (DSC)*, 2018.

[2] M. Andoni *et al.*, “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” vol. 100, pp. 143–174.

[3] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of Trust: A decentralized blockchain-based authentication system for IoT,” *Computers & Security*, vol. 78, pp. 126 – 142, 2018.

[4] O. Novo, “Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT,” *IEEE Internet of Things Journal*, vol. 5, no. 2, 2018.

[5] Linux Foundation, “Hyperledger Sawtooth,” accessed: 2019-06-14. [Online]. Available: https://sawtooth.hyperledger.org/docs/core/releases/1.0/introduction.html

[6] L. Gerrits, R. Kromes, and F. Verdier, “A true decentralized implementation based on iot and blockchain: a vehicle accident use case,” in *2020 International Conference on Omni-layer Intelligent Systems (COINS)*, 2020, pp. 1–6.

[7] Ameli, “Rapport annuel 2017,” accessed: 2021-05-17. [Online]. Available: https://www.ameli.fr