Wallance, an Alternative to Blockchain for IoT

Loïc Dalmasso, Florent Bruguier, Pascal Benoit, Achraf Lamlih
LIRMM
University of Montpellier, CNRS
Montpellier, France
firstname.name@lirmm.fr

With the concepts of “Internet of Things” (IoT) and “Internet of Everything” (IoE), connected devices overwhelm our society in many areas such as smart cities, environment, industries, etc. These devices, such as sensors or actuators, interact together and with their environment, assuming that anything can be connected to the global network. However, this hyper-connectivity and this omnipresence may potentially represent a huge privacy and security threat. Consequently, over the inherent required needs to secure IoT devices, communications and more generally, their interactions on the network, must be trusted.

In the classic client-server architecture, the server is in charge to receive/transmit information to clients but also to handle the security of the network. e.g. ensure the validity of a transaction. In this model, the network security relies on the server capacity to handle attacks and all participants have to trust the server as the central authority. Recent scandals regarding the personal data privacy show that this model cannot be safe. The weakness of the previous model is its central authority. To overcome this issue, the distributed network architecture is an interesting solution, where each participant on the network is directly connected to some others by a Machine-to-Machine (M2M) protocol. Thanks to that, information is directly transmitted to one participant to another, without a third party such as server. However, there is no standard to secure interactions and ensure the trust in such a system.

According to the state of the art, the blockchain approach brings many benefits in terms of reliability and security. It avoids a single point of failure, there is no involved third party and all validation processes are done by the network itself. Even if blockchain is a very promising system to ensure the trust in a distributed network, it requires heavy resources utilization such as computing power, energy consumption and storage capacity that are not at all available in IoT end-node devices.

Because of the lack of a suitable solution to secure decentralized IoT infrastructure, we developed our own protocol named Wallance described in Fig. 1, to ensure the trust between devices while taking into account constraints such as memory, computing power and energy. All source files are available on GitHub at https://github.com/WallanceProject. Since the aim of an IoT network is to connect everything to share data and create services, each data brings added value and enriches the network. In the same way as people post information on social network, IoT devices demonstrator share data to each other and they are rewarded for their sharing, in DCoin (Data Coin), the virtual currency of our network. With their coins, devices get the right to access resources/services e.g. maintenance service, energy. Since there is no central authority, all remunerations and accesses to services are controlled by the network itself through a consensus protocol based on a majority vote: to access to a resource/service, a request has to be validated by the majority of the network.

![Fig. 1. Wallance interaction scenarios](image1)

Beyond the concepts, it is essential to experiment and compare distributed protocols in real environment. For this purpose, we set up an IoT prototyping platform shown in Fig. 2. We can evaluate performances such as the energy consumption, the scalability (the number of handled transactions per second), the consensus delay, and the storage utilization, regarding the number of connected devices. In addition, our platform allows to perform security and robustness evaluation, by implementing attack in real conditions. Finally, to provide a fully customizable environment, different programming languages are supported such as C/C++, Python, etc.

Our IoT platform is composed of 48 Raspberry Pi3 Model B+ as IoT devices, connected to the same network through 2 TP-Link Archer C50 routers. 23 Raspberry are connected over Ethernet by a Cisco Catalyst 1900 switch and the remaining ones over WiFi 2.4GHz: 7 on the main router and 18 on the access point router. Additionally, a PC is used as a user-friendly interface to interact and visualize all interactions in real-time and to inject faults for the security evaluation purpose. Regarding the Wallance protocol, the interface shows all Raspberry’s wallets (containing their DCoin) and purchase services on behalf of selected Raspberry, such as the coffee service for the demonstrator purpose. The next step is to extend our platform with more Raspberry and to evaluate performances and robustness of Wallance in larger network.

![Fig. 2. IoT prototyping platform](image2)