Work in Progress-IoT Devices Sharing System Using Smart Contract

WENTAO TANG[†1]   KENJI HISAZUMI[†2]

Abstract: The development of Internet of Things has brought a large number of IoT devices. For both individuals and companies, it will be a big expenditure to purchase all IoT devices. This work in progress hopes to build a decentralized IoT devices sharing system based on smart contracts, which can eliminate the need of third-party for management and certification. To achieve this, we hope to use computers in different rooms or offices as nodes and miners to form a private blockchain network and deploy smart contract on it to supervise the user's identity, sharing process and rent payment. Considering the distributed characteristics of the blockchain network, we believe the entire process is credible. In this paper, we will make an introduction of the framework and interaction of our system.

Keywords: IoT, Smart Contract, Blockchain, Devices Sharing.

1. Introduction

Thanks to the rapid advance of communication and networking technologies, a growing number of objects (sensors, actuators, and smart devices) are being connected to the Internet nowadays, leading to the concept of the Internet of Things [1].

Usually, there are more than ten devices in one Smart House, and for places like office spaces in office buildings or school research rooms, more devices are needed [2]. Let us consider that buying all the devices will be a big expense. It will be a good idea to rent and share some devices between different rooms or offices, such as printers, sweeping robots, and so on.

However, due to security considerations, a system managed by a credible third party is usually required to process and supervise device rental and rent payment, which will also bring new expenses.

On the other hand, blockchain, which gives way for many different people or computers to agree on something even though they don't know or trust each other and allows the exchange and storage of digital assets without the need for third-party oversight, is becoming more and more popular [3]. Therefore, we hope to build a decentralized system to realize devices sharing by rental with blockchain and smart contracts, the program on the blockchain.

This paper will introduce this system, which can realize the functions of user authentication, rental management, and rent payment. At the same time, it will store transaction records in the blockchain and ensure credibility without a third party.

2. Related Work

In this section, we plan to introduce the concepts that will appear in this paper briefly.

Blockchain: A blockchain, also called a distributed shared ledger, is an immutable database of records secured by cryptography [4]. In our framework, blockchain contains blocks of transactions and smart contracts with each block containing the hash of its previous block. Each node in the network may have a local copy of the entire blockchain to ensure data integrity and tamperproof.

Ethereum platform: Our framework is based on the Ethereum smart contract platform, which is an open software platform built on blockchain technology that enables developers to build and deploy decentralized applications [5].

Smart contract: A smart contract is a special account with associated code and data on Ethereum [6]. The Ethereum address of a contract can be used in a transaction as the recipient, sending funds to the contract, or calling one of the contract's functions. A smart contract usually provides many functions for other accounts to interact with it.

3. Devices Sharing System Framework

The overview of the framework is shown in figure 1. Here, different office rooms provide one or two computers as Ethereum nodes. Each node has an Ethereum account and runs an Ethereum client to form a private blockchain network. The user management contract (UMC) will then be deployed on the network by one of the nodes.
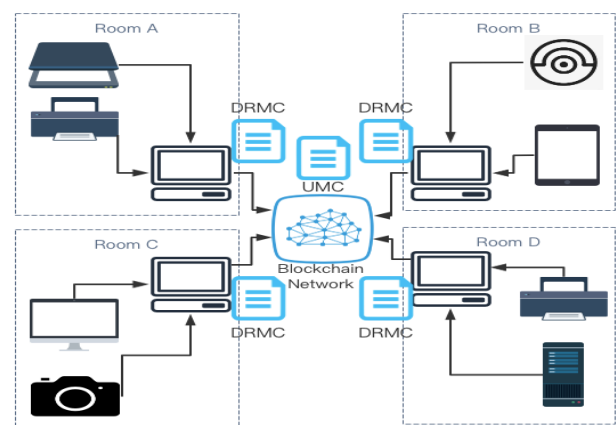

Figure 1. Overview of our framework

Each node, including the new node that wants to join the blockchain network, first needs to register for its own Ethereum account in the private blockchain network through UMC. Then

---

†1 Graduate School of Information Science and Electrical Engineering, Kyushu University

†2 Faculty of Information Science and Electrical Engineering, Kyushu University

members of each office can deploy the devices rental management contract (DRMC) for their devices on this node to rent devices out and use the function of DRMC deployed by other users to rent devices in. For each DRMC, it will be linked with UMC during deployment so that the information of registered users can be obtained from UMC to verify the identity. And all the cost will be paid in Ether, the digital money for Ethereum.

At the same time, each node will also play a miner's role to process transactions on the private chain.

4. Smart contract system

4.1 User management contract

The primary function of UMC is to register a new account for the private blockchain network. To ensure security, we intend to register new accounts through voting by all users.

Any new Ethereum account that wants to join the private chain can apply for registration by calling the smart contract function to trigger the registration event. At this time, all the accounts in the private chain can vote for the request within the specified time. If more than half of the users agree to the request, the contract will recognize the request and register this account as a private chain user.

4.2 Devices rental management contract

The function of the DRMC is to manage the process of devices rental and rent payment. In order to allow devices providers to get the most benefits, we hope to rent devices by auction.

After registration, the account can deploy its own DRMC or bid for other accounts' contracts. We give an overview of what users can do during the auction in figure 2, and what users should do after winning the auction in figure 3.
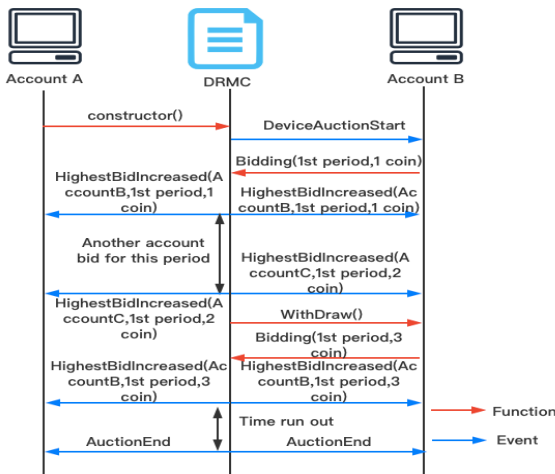
Figure 2. Sequence diagram for bidding

When the device provider deploys his own contract, he enters relevant information through the constructor, including the starting price, the duration of the auction, the deposit amount, and a timetable for using the device.

After the contract is deployed, other accounts can bid for any one or several usage periods. To prevent the bidder from just not sending the money after they won the auction, the only way is to make them send it together with the bid [7]. If the highest bid is raised, the previously highest bidder can get their money back with the function.
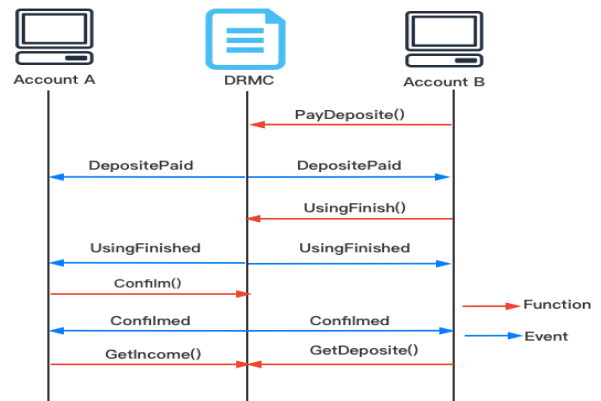
Figure 3. Sequence diagram after won the bidding

After winning the auction, the account needs to pay a deposit first and use the device within the specified time. If overtime or equipment is damaged, the deposit paid cannot be recovered.

For all the functions in DRMC, when called, the contract will confirm whether the caller has completed the registration through the UMC.

5. Conclusion and future work

In this paper, we proposed a smart contract-based framework on Ethereum, which includes one UMC for all users and one DRMC for each device, to implement decentralized and credible IoT devices sharing system without third party oversight.

Next, we plan to complete a case study for this work in progress to demonstrate the feasibility of the proposed framework in realizing decentralized and credible IoT devices sharing and do some research on the efficiency and cost of this framework.

Reference

[1] I. Yaqoob, E. Ahmed, I. A. T. Hashem, and A. I. A. Ahmed, "Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges", in IEEE Wireless Commun., vol. 24, no. 3, pp. 10-16,2017.

[2] T. Zou, H. Feng, K. Hisazumi, and A. Fukuda, "A Code Generating and Verification Method from DSM Language for Secure IoT Applications", in 2019 Information Processing Society of Japan, pp. 125-126, 2019.

[3] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, "Decentralized document version control using Ethereum blockchain and IPFS", in Computers and Electrical Engineering, pp. 183-197, 2019.

[4] K. Kostal, P. Helebrandt, M. Bellus, and M. Ries "Management and Monitoring of IoT Devices Using Blockchain", in Sensors, Vol 19, Iss 4, p 856, 2019.

[5] "WHAT IS ETHERUM?". https://ethereum.org/en/what-is-ethereum/, (accessed 2020-09-23).

[6] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart Contract-Based Access Control for the Internet of Things", in IEEE Internet of Journal IEEE Internet Things J. Internet of Things Journal, IEEE. 6(2), pp. 1594-1605, 2019.

[7] "Solidity by Example". https://solidity.readthedocs.io/en/v0.6.10/solidity-by-example.html, (accessed 2020-09-23).