Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 198 (2022) 448–453

Procedia Computer Science

www.elsevier.com/locate/procedia

International Workshop on Internet of Smart Things (IST 2021)
November 1-4, 2021, Leuven, Belgium

Scalable Access Control Scheme of Internet of Things Based on Blockchain

Wei Xiang[a]*, Zhang Yuanyuan[b]

[a]*Heibei Vocational College of Arts and crafts,Baoding City ,Hebei Province,071051,China*
[b]*Shijiazhuang Engineering Technology School,Shijiazhuang City, Hebei Province,050061,China*

Abstract

With the development of Internet of things (IoT) technology, a large-scale, heterogeneous and dynamic distributed IoT environment has gradually formed between different IoTs. In order to solve the scalability problem of restricted device access management in the Internet of things, a distributed access control system model of the Internet of things based on blockchain technology is proposed. The system model adopts a single smart contract, which simplifies the whole process in the blockchain network and reduces the communication overhead between nodes. According to the simulation results and evaluation, it is proved that the solution has good scalability.

Keywords: Blockchain; Internet of things; Access control; Smart contract; Scalable

1. Introduction

The Internet of things has produced a large amount of data, which contains a lot of personal privacy. Once this privacy information is leaked, it will bring huge losses to users. As one of the cornerstone technologies of data protection, access control can ensure that data can only be accessed by users with corresponding permissions [1].

* Corresponding author. Tel.: 17734561268.
E-mail address: 27841205@qq.com

10.1016/j.procs.2021.12.268

Therefore, the access control mechanism under the Internet of things has become one of the important research contents of Internet of things security and privacy protection.

Blockchain is a decentralized distributed technology, which technically solves the security problems brought by the trust based centralized model. Therefore, researchers combine blockchain and access control as the key technology of Internet of things data protection.

2. Related work

Some preliminary work has been done in blockchain based access control. Taking full advantage of the decentralized, tamper proof, traceable and smart contract characteristics of blockchain, the blockchain is used as a trusted entity to build an access control model [2-14]. Firstly, researchers preliminarily explored the feasibility of designing a new framework on the blockchain. For example, literature [2-6] proposed their redesigned access control models on the blockchain. Then, researchers put forward a more detailed access process rather than limited to the framework: Zhang et al. [7] proposed a static access control model; Ding et al. [8] proposed an attribute based access control method for the IoT; Ramachandran et al. [9] proposed a management method of scientific data sources; Ali et al. [10] proposed an access control model under the Internet of things, and put forward requirements for event and query basic authority delegation. Furthermore, researchers have solved the key problems in the Internet of things environment: Dorri et al. [11] proposed a method to use token to alleviate the huge problems of blockchain existence time, computing and storage overhead; Lin et al. [12] solved the problem of fine-grained access; The model of Alphand et al. [13] is flexible; The model proposed by Ma et al. [14] can be accessed across domains. Although many studies have been done on the combination of blockchain and access control, these access control models are generally not scalable. Therefore, this paper proposes a scalable access control system model of Internet of things based on blockchain.

The main work of this paper is as follows: in order to solve the scalability problem of Internet of things device access management, a distributed access control system of Internet of things based on blockchain technology is proposed. The solution defines a new node of the management center to request access control information from the blockchain on behalf of the Internet of things devices. It involves a smart contract that defines all operations allowed in the access control system and cannot be deleted from the system. The scheme is evaluated in the actual Internet of things scenario, and the results show that the blockchain technology can be used as an access management technology in a specific scalable Internet of things scenario.

3. Extensible access control system model

3.1. System model

The model structure of extensible access control system is shown in Figure 1, including six different components.

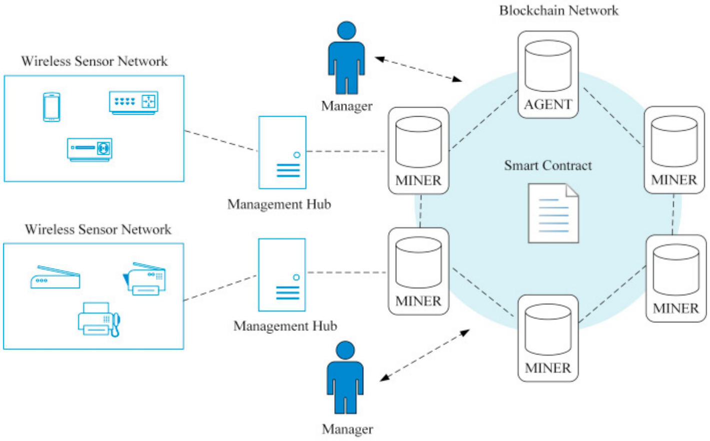

Fig. 1. Extensible access control system model

(1) Wireless sensor network: this is a communication network that allows limited connections in applications with limited power and optical requirements. IoT devices do not belong to blockchain networks. Therefore, all devices must be globally and uniquely identified in the blockchain network. The public key generator provides a feasible solution to the problem of generating acceptable and unique random numbers. Using the existing Internet of things encryption technology will automatically create a public key for each device. Therefore, enforcing an encrypted connection will ensure a unique identifier.

(2) Manager: an administrator is an entity responsible for managing access control permissions for a group of IoT devices. The administrator in this scheme does not need to continuously connect to the blockchain network, which helps to reduce the use of its hardware resources. The registration of IoT devices must be under the control of the administrator, who can define specific access control permissions for them.

(3) Agent node: the agent node is a specific blockchain node in the architecture, which is responsible for deploying the only smart contract in the system. Once the smart contract is received in the blockchain network, the proxy node will receive an address that identifies the smart contract in the blockchain network.

(4) Smart contract: the access management system proposed in this paper is controlled by the operation defined in a single smart contract. This smart contract is unique and cannot be deleted from the system. After the transaction triggers the operation, the proxy node will maintain the global accessibility of the transaction information. Smart contracts and their operations are also globally accessible.

(5) Blockchain network: the blockchain network in this system is a private blockchain. Because all elements of the prototype have larger dimensions, it can provide more reliable results for the evaluation system. However, in the actual scenario, the public blockchain should be used to promote the application of the solution.

(6) Management hub: as mentioned earlier, IoT devices do not belong to blockchain networks. Most IoT devices are greatly limited in terms of CPU, memory and battery, which limits IoT devices from becoming part of the blockchain network. Therefore, choose to introduce a node called the management center. The management center is an interface that can convert the information encoded by the IoT device in the constrained application protocol (COAP) message into a json-rpc message understandable by the blockchain node. The management center is directly connected to the blockchain node miner. Multiple sensor networks can be connected to one management center node, and multiple management center nodes can be connected to the same blockchain node. IoT devices can only request access to information from the blockchain through the management center.

3.2. System interaction

This section will explain the different interactions between different components in the architecture. As shown in Figure 2, the system interaction can be divided into four different stages.

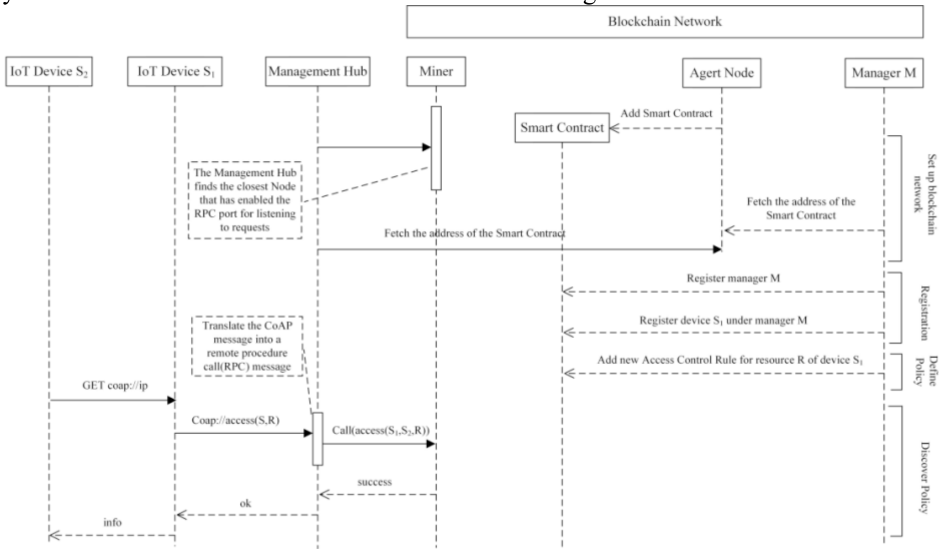
Blockchain Network
IoT Device S_2
IoT Device S_1
Management Hub
Miner
Agert Node
Manager M
Smart Contract
Add Smart Contract
The Management Hub finds the closest Node that has enabled the RPC port for listening to requests
Fetch the address of the Smart Contract
Fetch the address of the Smart Contract
Set up blockchain network
Register manager M
Register device S_1 under manager M
Registration
Add new Access Control Rule for resource R of device S_1
Define Policy
Translate the CoAP message into a remote procedure call(RPC) message
GET coap://ip
Coap://access(S,R)
Call(access(S_1,S_2,R))
success
ok
info
Discover Policy

Fig.2. interactive process of network setting, registration, definition and policy discovery

(1) Network settings: create an access management system in the blockchain network. When creating a blockchain network, the proxy node deploys the smart contract into the blockchain network. The smart contract defines all operations of the access control management system. Once it is received in the blockchain network, the proxy node will receive the address corresponding to the smart contract. This address is used to identify the smart contract in the access management system. Other components of the blockchain network need the address of the smart contract to interact with it.

The management center will connect to the nearest available node in the blockchain network, that is, the miner node in Figure 2. The miner has a copy of the blockchain. In addition, the miner allows the remote procedure call (RPC) port to listen for requests and allows central administration to connect to the port.

(2) Registration: any blockchain node in the access management system can be registered as an administrator. As long as the blockchain node obtains the address of the smart contract, it can independently register as an administrator and send the transaction to the function register manager defined in the smart contract. When the transaction is connected to the blockchain, the administrator will receive its registration address, which will identify the administrator in the access management system. The management node can register IoT devices under the control of the administrator. The administrator will receive the address of the registered device, which is used to identify the device in the access management system.

(3) Management modification: as mentioned earlier, each IoT device must belong to at least one administrator. In addition, the system supports multiple administrators to control the same device. There are many ways to transfer management control from one administrator to another, or add or delete multiple administrators from the system. Each administrator node in the system can remove its own administrator identity, but other administrators cannot be deleted.

One of the advantages of this solution is that because all operations in the system are defined and executed using a single smart contract, and administrators do not need to interact with each other, it is a simple process to transfer the management control of IoT devices. The administrator only needs to know the address of the device and smart contract to modify the management relationship.

(4) Policy definition: administrators can define access control rules for IoT device resources, which can be defined in a variety of ways. Because the devices that have access to specific resources are listed in the implemented permissions, administrators need to know not only the address of the devices they control, but also the address of the devices that have access to them. Administrators can use this information to create a smart contract oriented transaction and enforce policies.

4. Simulation experiment

Ethereum is one of the most popular blockchain based distributed computing platforms. This section will evaluate how the introduction of management center nodes into the blockchain system affects the overall delay of the architecture. Along this idea, evaluate whether the integration of datagram transport layer security (DTLS) library and the connection between IoT devices and management center nodes will become the technical limitations of this method.

(1) Experimental setup

The experiment is equipped with Intel Core i7- 950@3.07 GHz Ubuntu-16.04 desktop. An open source application container engine Docker and an image named vertigo / Ethereum are used. The image client-go client is implemented in the Golang programming language derived from Ethereum / client-go. Vertigo has been slightly modified to make it easier to run private Ethereum network. Internet of things devices run a modified version of LibCOAP (LibCOAP is the C language implementation of COAP protocol) library on the same computer.

In order to measure the experiment, a benchmark tool named CoAPBench is used, but the function of this tool is limited for the test purpose of this article. After modification, CoAPBench can send post, put and delete messages and allow the payload to be specified in the request message.

(2) Performance verification

The experiment evaluates how the introduction of the management center node into the blockchain system affects the delay of access control operation in the system, as shown in Figure 3.

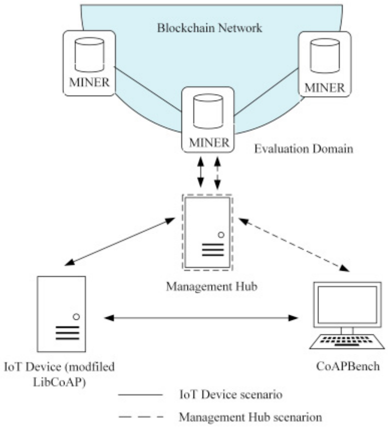

Fig.3. evaluation domain

First, independently evaluate the performance of the management center, that is, a group of virtual IoT devices in the CoAPBench tool are directly connected to the management center. In this scenario, the virtual client is configured to request access information of one IoT device to resources in another IoT device. Once the management center receives the request, it will obtain information from the blockchain network through RPC calls and return the response to the virtual client.

In the second scenario, the performance of IoT devices connected to the management center node is evaluated, that is, a group of virtual IoT devices from the CoAPBench tool request resource information of another IoT device, which is connected to the management center. In this scenario, all IoT devices are also integrated with the DTLS library. Once authorized from the blockchain network and proxy to the IoT device through the management center, it will grant or reject the information of the resource accordingly.

In both scenarios, the blockchain network grants all requests to all resources. In addition, the tests in the two scenarios are performed on different numbers of concurrent clients. Each test is measured 5 times for 30 seconds each time, and the average value is calculated. The number of concurrent clients is between 1 and 10000.

Fig.4. (a) shows the test results of two scenarios. Note that both Fig. 4. (a) And Fig. 4. (b) Use logarithmic scales. The first scenario shows how the throughput of the management center increases from 500 requests per second to a stable throughput of 950 requests per second, and 10 concurrent clients reach the maximum capacity. After that, the performance will slowly decline, which is directly related to the number of timeout request messages, as shown in Fig. 4. (b).

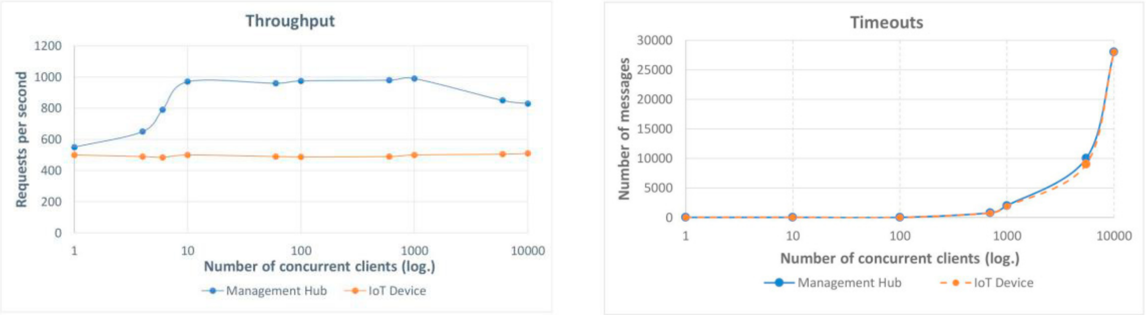

Fig. 4. (a) Throughput executed independently in the management center and the IoT device requesting information from the management center; (b) The number of timeout request messages that executed the test

Throughout the test period, the throughput of the second scenario stabilized at 500 requests per second. In this scenario, all concurrent clients request resource information from a single IoT device. Therefore, the delay between the management center and a single Internet of things client limits the overall performance of the scenario. Generally speaking, the limiting factor of both scenarios is the delay in obtaining access control information from the blockchain network.

The system bears the delay overhead of publishing access control information on the blockchain network, which has a negative impact on the system performance. Nevertheless, the management center can achieve the best performance at 900 requests per second without more than 1000 concurrent clients. Considering that wireless sensor network can connect multiple management center nodes, the performance of management center is acceptable. Considering that Internet of things devices are resource limited and in many cases, hardware capability is a greater limiting factor than software, the performance of the system is generally acceptable in terms of scalability.

5. Conclusions

In summary, this paper studies the scalable access control of Internet of things based on blockchain. In order to solve the scalability problem of access management of billions of restricted devices in the Internet of things, a distributed access control system of the Internet of things based on blockchain technology is proposed. Because many restricted networks can be connected to the blockchain network at the same time through a specific node called the management center, the system is scalable. Different management center nodes are distributed around the whole blockchain network and connected to the restricted network in different ways. Its universality provides good flexibility for the scheme. According to the simulation results and evaluation, it is proved that the system has good scalability.

This paper mainly studies the application of blockchain technology in the access control system of the Internet of things. Although some achievements have been made, there are still many theoretical and application problems to be further studied in the performance optimization of the system: (1) how to improve the efficiency of hardware equipment and reduce the cost of blockchain storage is a problem worth studying in the access control of the Internet of things;(2) Scheme testing should be carried out in the real Internet of things field to create standards for blockchain based Internet of things access management.

References

[1] Fang Liang, Yin Lihua, Guo Yunchuan and Fang Binxing. (2017) “Research review on Key Technologies of attribute based access control.” *Journal of Computer Science* **40**(**7**): 1680-1698.

[2] Hossein Shafagh,Lukas Burkhalter,Anwar Hithnawi and Simon Duquennoy. (2017) “Towards Blockchain-based Auditable Storage and Sharing of IoT Data.” *Cloud Computing Security Workshop*.

[3] Mei Ying. (2017) “Simplification model construction of Internet access control based on blockchain.” *Journal of Communication University of China* **24**(**5**):7-12.

[4] Zyskind,Nathan and Pentland. (2015) “Decentralizing privacy:using blockchain to protect personal data.” *Proceedings of the 2015 IEEE Security and Privacy Workshops*. Piscataway:IEEE,180-184.

[5] Rifi,Rachkidi and Agoulmine. (2017) “Towards using blockchain technology for IoT data access protection.” *Proceedings of the IEEE 17th International Conference on Ubiquitous Wireless Broadband*. Piscataway:IEEE,1-5.

[6] Chethana Dukkipati,Yunpeng Zhang and Liang Chieh Cheng. (2018) “Decentralized, BlockChain Based Access Control Framework for the Heterogeneous Internet of Things.” *Attribute-Based Access Control.*

[7] Zhang,Kasahara and Shen. (2019) “Smart contract-based access control for the Internet of things.” *IEEE Internet of Things Journal*, **6**(**2**):1594-1605.

[8] Ding, Cao, and Li. (2019) “A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT.” *IEEE Access*, 38431-38441.

[9] Ramachandran,Kantarcioglu. (2019) “Using blockchain and smart contracts for secure data provenance management [EB/OL].” *https://arxiv. org/pdf/1709*. 10000. pdf.

[10] Gauhar Ali,Naveed Ahmad,Yue Cao and Qazi Ejaz Ali. (2019) “Blockchain based permission delegation and access control in Internet of Things (BACI).” *Computers & Security.*

[11] Dorri,Kanhere and Jurdak. (2017) “Blockchain for IoT security and privacy:the case study of a smart home.” *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops*. Piscataway:IEEE,618-623.

[12] Chao Lin,Debiao He,Xinyi Huang and Athanasios V. Vasilakos. (2018) “BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0.” *Journal of Network and Computer Applications*.

[13] Alphand,Amoretti and Claeys. (2018) “IoTChain:a blockchain security architecture for the Internet of things.” *Proceedings of the 2018 IEEE Wireless Communications and Networking Conference*. Piscataway:IEEE,1-6.

[14] Ma,Shi and Li. (2019) “Privacy-oriented blockchain-based distributed key management architecture for hierarchical access control in the IoT scenario.” *IEEE Access*,7:34045-34059.