Data Sharing Model of Internet of Things Based on Blockchain

Nana Liang1,*

1Henan industry and information technology professional college, Henan, Jiaozuo, 454000

*Corresponding author e-mail: liang-na@163.com

Abstract. Blockchain technology and Internet of Things technology are two new technologies formed in the current transmission of information technology. In the implementation of its technical control, it can scientifically control the information sharing work and realize the artificial adjustment of the transmission control of the Internet of Things technology. In this paper, research on the Internet of Things data sharing model based on block chain with a view to provide guidance to the security of Things data sharing technology under the block chain. In this paper, Hyperledger Fabric block chain platform-based platform, proposed a block-based chain of IOT data sharing model, security and data privacy is an enhancement, obtained by the performance of the test model. Throughput is maximized when the write transaction sending frequency is 100 TPS and the query transaction sending frequency is 250 TPS. The maximum write throughput is 60 TPS, which is better than Bitcoin and Ethereum on the public chain, which proves the feasibility of the model implementation. This model can achieve storage and sharing without the help of a third-party centralized organization, and directly establish trust between participants, which can ensure the safe sharing of data.

Keywords: BlockChain, Internet of Things, Data Sharing, Model Research

1. Introduction

In recent years, the rapid development of Internet of things market, BLE, Zigbee, NFC, WiFi, LoRa, NB-IoT, 5 g rapid development of Internet communication technologies such as cloud services universal application, big data, such as artificial intelligence technology matures, for data collection, transmission, storage, analysis and use with the full protection, the value of mining data behind no longer distant and [1-2]. Technological advances also mean new challenges. A large amount of data associated with the physical world on the Internet, make the user's personal privacy is faced with great
threat, safety input greatly increase [3]. Internet of things have very strong heterogeneity, the data collected by different network often confined to its own exclusive domain, between each other is difficult to secure sharing, and the problem of data island. Even reached cooperation between organizations within the scope of the legal share data, often need to build credible centralized Shared institutions [4-5]. Centralized organization construction and the maintenance cost, however, need to be solely responsible for the management of the equipment, data storage and transmission, once it fails, the system as a whole will be paralyzed. In addition, the centralized organization is not transparent to participants, too much power, internal or external malicious behavior may cause data to be tampered with [6].

With the development and popularization of COINS, block chain technology application and the research presents the explosive growth, by governments, technology companies, research institutions attention [7]. Block chain technology has been extended to the financial, trade, inquiry, the Internet of things, resource security, entertainment and medical health and other fields, and get the preliminary application [8]. Due to its technical features of decentralization, reliable database, de-trust, transaction anonymity, collective maintenance and open source programming, blockchain can enable participants to build mutual trust and realize the reliable transmission of value without centralized institutions. This advantage is suitable for improving the single point of failure, system security and other problems in the current management of the Internet of things [9-16].

Based on Hyperledger Fabric, this paper proposes a data sharing model of Internet of things based on block chain. For security and data privacy, through performance test of the model, prove the feasibility of the model. Without relying on a single trusted centralized institution, the model can directly establish trust between participants and ensure data security sharing.

2. Method

2.1. Internet of Things Data Information Sharing Under the Application of Blockchain Technology

Block chain technology is a distributed control technology, which is a new technology control mode formed in the process of information technology transfer. For block chain technology application, for the control of distributed information transfer mode is more important. Through the control of distributed architecture and transformation, in the process of information sharing, risk factor analysis of the existing in the information exchange, eliminate safety hidden danger in time. In addition, in the process of block chain technology application and Internet of things information technology sharing, information sharing control of information transmission can be realized through information technology improvement, which improves the control effect of information transmission.

The security basis of blockchain is to use digital encryption technology to guarantee, while digital encryption technology is to use cryptographic algorithm to solve the security problem of data. The digital signature technology is to encrypt the digital news to get signature. Common digital signature algorithms include elliptic curve digital signature algorithm, whose verification formula is:

\[ s \times (k \times G) = H_w \times G + r \times (pk \times G) \rightarrow s \times R = H_w \times G + r \times P \]  

(1)

Agent technology is a re-encryption key ciphertext translation mechanism between, can leak without the data owner's private key, the ciphertext data sharing cloud, the agent is re-encryption
algorithm formula:

\[ m = \frac{e(g, g)^{y} \cdot m}{e(g, g)^{y} \cdot e(g^{ry}, g)} = \frac{e(g, g)^{y} \cdot m}{e(g, g)} \]  

(2)

In order to obtain data sharing, data ownership control access rights management.

2.2. Hyperledger Fabric

The Hyperledger Fabric project began as an enterprise application scenario. Is a platform that provides blockchain solutions that developers can expand upon. Unlike public chains such as bitcoin and ethereum, it has strict permission and identity management schemes, focusing on transaction security and modular design. Key components of Hyperledger Fabric include: client, node, sorting service, MSP, chain code, and channel. The client can initiate transactions in the network, listen to messages, update configuration, start-stop nodes and other functions. Peer node including endorsement and confirm functions. Sorting collected legal services for trading in a certain time in order to sort, can choose the degree of decentralization. MSP defines a series of standard specification, and check the digital certificate in the node, sorting, services, channels, and other components in the configuration file contains information authorized organization of MSP. Chain code is also known as "smart contract" on other blockchain platforms. HyperledgerFabric provides system chain code and user chain code. Channel can be thought of as built on block chain network subnet, block chain data access management.

3. Experiment

This design model layer using block chain management services for distributed network storage and use data to make improvements. Enhanced data security and privacy aspects of the design, the design of a new gateway, the certificate management module, and a data receiving and processing module consisting Fabric SDK, cooperate with each other so that three things device interact with block chain network. Due to security reasons, this model will share the data channel called "data channels" and proposed "log channel" for every query data log channel through the completion of the call chain codes, once the data leaks, view the log channel recording , It can be traced to weaknesses and the range of possible leakage. Data Privacy design, if the relevant members are involved in the same project, you can create a separate channel for these members. Channel has its own books and access policies, internal channel members can access external completely isolated. The test environment for this experiment is shown in Table 1.

| Project       | Configuration                     |
|---------------|-----------------------------------|
| CPU           | 2.6 GHz Intel Core i5             |
| Storage       | 8 GB memory,256 GB SSD           |
| Operating system | Mac OS10.13.6                   |

Table 1. Test environment
4. Discussion

4.1. Performance Testing and Analysis

The performance testing tool uses the Hyperledger Caliper framework to test the blockchain network running on a single host, including 4 nodes belonging to 2 organizations, 2 MSPs, 1 sorting service using SOLO consensus, 5 clients, and above. The components belong to one channel. The test method is to send 5000 transactions to the blockchain network. Observe the changes in the average delay and throughput of the system under different transaction sending frequencies. The results are shown in Figure 1.

![Figure 1. Query performance](image)

It can be seen that the average delay increases as the transaction sending frequency increases. The maximum write throughput is 60 TPS, which is better than Bitcoin and Ethereum on the public chain. The throughput write transaction is 100 TPS, and the query transaction frequency is 250 TPS. If you use high-performance servers to run each component separately, you can further shorten the time-consuming operations such as signing and encryption. Although the blockchain network contains only 4 nodes, due to the endorsement strategy, it can still ensure that the network is decentralized and tamper-proof. Tampering with data will cause the block hash value to change. Comparing the ledgers and transaction signatures of different nodes can quickly find the tampered place, and the update based on tampered data will cause the endorsement results of different members due to the limitation of the
endorsement strategy Inconsistent, the transaction will be deemed invalid.

4.2. Analysis of Resource Consumption

For the set of tests with the largest write throughput, record their resource consumption, as shown in Table 2.

| Component name | Average memory usage (MB) | CPU average usage (%) | Disk writes (MB) |
|----------------|---------------------------|-----------------------|-----------------|
| Node 1         | 209.3                     | 28.41                 | 32.7            |
| Node 2         | 180.9                     | 24.46                 | 32.7            |
| Node 3         | 184.5                     | 28.44                 | 32.7            |
| Node 4         | 171.7                     | 21.27                 | 32.7            |
| Sorting service| 37                        | 13.36                 | 23.1            |

It can be seen from Table 2 that the resources consumed by each component are not high, and the realization of the model can be satisfied under the premise of ensuring throughput and delay. The nodes used for endorsement and confirmation take up more resources, and the actual deployment should pay attention to enhance the performance of the server where such components are located.

5. Conclusion

In the security management of IoT data sharing under the application of blockchain technology, due to the large amount of data in the field of IoT and the difficulty of sharing between different organizations, there are differences in the construction of blockchain technology application in the implementation of data sharing security management. Based on the Hyperledger Fabric blockchain platform, this paper proposes a data sharing model for IoT based on blockchain. It proposes enhanced and improved methods for security and data privacy, analyzes the security and feasibility of the big data sharing model, and proves the feasibility of the model implementation by testing the performance of the simplified model. With the present model, data between different organizations can implement things stored and shared in a third party without the aid of centering means, it is possible to improve the efficiency of data transfer things. Implemented so as to achieve block chain technology transfer and data sharing things purposes.

References

[1] Xue T F, Fu Q C, Wang C, et al. A Medical Data Sharing Model via Blockchain[J]. Zidonghua Xuebao/Acta Automatica Sinica, 2017, 43(9):1555-1562.

[2] Zhang G, Li T, Li Y, et al. Blockchain-Based Data Sharing System for AI-Powered Network
Operations[J]. Journal of Communications and Information Networks, 2018, 3(3):1-8.

[3] Yang M , Margheri A , Hu R , et al. Differentially Private Data Sharing in a Cloud Federation with Blockchain[J]. IEEE Cloud Computing, 2018, 5(6):69-79.

[4] Onik M M H , Kim C S , Lee N Y , et al. Privacy-aware blockchain for personal data sharing and tracking[J]. Open Computer Science, 2019, 9(1):80-91.

[5] Xuan S , Zhang Y , Tang H , et al. Hierarchically Authorized Transactions for Massive Internet-of-Things Data Sharing Based on Multilayer Blockchain[J]. Applied Sciences, 2019, 9(23):5159.

[6] Ullah I , Sultana T , Javaid N . Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices[J]. Applied Sciences, 2020, 10(2):488.

[7] Mollah M B , Azad M A K , Vasilakos A . Secure Data Sharing and Searching at the Edge of Cloud-Assisted Internet of Things[J]. Cloud Computing, IEEE, 2017, 4(1):34-42.

[8] Banerjee S S , Hemphill T , Longstreet P . Wearable devices and healthcare: Data sharing and privacy[J]. The Information Society, 2018, 34(1):49-57.

[9] Wang X A . PRE+: Dual of Proxy Re-encryption for Secure Cloud Data Sharing Service[J]. International Journal of Web and Grid Services, 2018, 14(1):1.

[10] Hu X , Tang C , Wong D S , et al. Efficient pairing-free PRE schemes for multimedia data sharing in IoT[J]. Multimedia Tools and Applications, 2018, 77(14):18327-18354.