Research on Privacy Protection Based on Block Chain in Internet of Things Network

Wang Chun¹, Chen Li*¹
¹ Wuhan Donghu University, Wuhan, Hubei, 430212, China
*Corresponding author’s e-mail: 29098854@qq.com

Abstract. The block chain technology has brought a dramatic change in the Internet of Things network, especially in personal privacy protection, due to the structural characteristics of decentralized, smart contract and immutability. This paper starts with the analysis of characteristics of block chain technology, further analyses the privacy protection problems in IOT network, then propose a personal data management system model to solve the problem.

1. Introduction

1.1 Brief introduction of block chain

Block chain is a distributed database that maintains a set of records in the form of blocks[1]. These blocks are transparent and can only be accessed by each block chain node, but cannot be deleted or modified. Blocks combine with each other to form a chain structure, and each block is linked to the previous block according to its hash value. Similarly, each block contains all the transaction information of the system and its transaction value, including the creation time and private key. Since the block chain is used in a P2P network, the communication between peers can only be carried out by broadcasting. Once a new node in the block chain is added and verified, it cannot be modified or deleted, it can be stored permanently, and thus the data will be more stable and reliable. The first block in the block chain is called Genesis, for any new block in the block chain database; it has only one path to Genesis. There are the three stages of development of the block-chain technology:

(1) Block chain 1.0 - Digital currency. As the name suggests it is a virtual currency represented by bitcoin, although there are many deficiencies, but it is the bud of the block-chain, and also a successful application of block chain technology.

(2) Block chain 2.0 - smart contracts. Smart contract can be defined as a computerized contract which characterizes the terms and conditions of a transaction between two entities. It is executed within the frame of chain code based on business model and resource definitions. The code allows the mutual settlement of contractual terms, and ensures that there is no alteration in every recording in the network. Hence, trust is assured and duplication is eliminated. [2]

(3) Block chain 3.0 – Decentralized. To decentralization is the node of the block chain to jointly maintain a peer-to-peer network without centralized management, the rights of any node is equal. It can apply to all fields of society, this technology replaces the trust in individuals or institutions required by traditional finance with the trust in the technology system, and human intervention will be difficult to work.
1.2 Brief Introduction of Internet of Things

The Internet of things (IOT) is a technology that has emerged only in recent years, for example, when we give an order online and receive a package, the process of package management is applied to the IOT technology. In recent years, this technology has been gradually developed in the many aspects, such as car, clothing, house furnishing and so on. The increased use makes it become more and more popular, but this technology has some similarities but different from the Internet. Not like the Internet data relies on input, the IOT mainly through sensors to obtain data, which makes the data is accurate and extensive, so the data protection of IOT should be pay more attention.

2. Research progress on the integration of Internet of Things and block chain

With the help of block chain, the information security problem including personal data storage, data access and data exchange can be well solved, the block chain technology can use some encryption and authentication strategies to ensure date security, it can also keep the personal data permanently, people can also make a subsequent inquiry.

2.1 Personal data storage

With the widely use of IOT devices, the number of personal data is increasing rapidly. Most IOT devices with the architecture of centralized network, how to keep data be stored safely becomes a difficult problem, at the same time to keep it integrity. The characteristics of decentralized and tamper proof of the block chain make it possible. At present, a lot of research has been applied in block chain technology for personal data storage.

![Personal data management system model](image)

Figure 1 Personal data management system model

Personal data storage is the management of personal sensitive data, nowadays cloud storage has become the choice of most individuals and enterprises, in which a third-party key with private...
information is used for data access. If the third party is not trusted, the privacy of the user will be disclosure. In order to solve the problems of cloud storage, we can build a security cloud storage system based on block chain technology, as shown in Figure 1.

The personal data are stored by cipher text in block chain through smart contract, at the same time the encrypted files are uploaded and stored in the cloud servers, which can only be decrypt by content key. Through the public key encryption processing authentication, the synchronization algorithm processes the data exchange between users and services, and verifies the license through the database authentication server. [3]

At present, there are also storage problems caused by data leakage, in order to solve them, the researchers proposed a method based on autonomous genetic algorithm and taboo search algorithm, which make the security of block chain network has been greatly improved. [4]

2.2. personal data access
As mentioned above, most of the user's personal data is stored in the data center on the cloud, through the centralized access method to control the data access with a stronger encryption scheme. Once a malicious node enters the system, it can access all the data, which may lead to a strong privacy leak and seriously threaten to the information security of users. What’s more, most of the services that receiving and applying for are mobile applications, a major security threat is that users need to grant a set of permissions when they are registering, with the permissions, these applications can continuously collect users’ personal data, everyone even has no idea how their data is accessed or collected. Thanks to the characteristics of block chain technology of decentralization, distrust and anonymity can be used to construct the system of data collection or access.

The system should ensure the owner of the data have the right to control their personal data, and the services as a visitor only has the authorized access rights, at any time, users can change their permission set and revoke access to previously collected data. Access control policies are secured on the block chain where only legitimate users are allowed to change them; therefore, it can effectively ensure the secure access of personal data.

At present, most of the database systems and enterprise information systems are based on the role-based access control technology which runs stably but not safely, but the simple role access control sometimes cannot meet the needs of actual access control. The role-based access control can be combined with attribute based access control which can integrated into the block chain through smart contracts, as shown in Figure 1. The data owner uploads the data to the database center in service center through encryption; sensitive private data can be uploaded directly to the block chain, and set appropriate access policies for the request access. Once someone wants to access the date, a corresponding permission request must be started through the smart contract, and the data access can only be carried out after the consent is obtained.

With the increasing of valuable data is generated by the use of IOT devices, users' demand for hierarchical access control is also increasing, the research shows that when the third party can't be confirmed to be completely trusted, the centralized management system cannot meet the need of access control services. However, using the distributed key management architecture based on block chain can improve the frequent requests. In order to better protect the access privacy, this structure uses fog computing to solve the problem of reduce latency, and use multiple block chains to realize transregional access services.

At the same time, in the traditional cloud storage system, the key and privacy data may be leaked out, in combination with block chain, the data owner can set the data access policies and the distribute the key to users. Through the combination and interaction with smart contract, the system can upload and update files with the transmission time is not limited, which improves the whole access control ability of the system.

2.3. personal data exchange
With the development of smart city of IOT, the demand for data is increasing, and the data exchange
has gradually entered in people's vision, the data owner can share and exchange their data in the special market. However, the current data exchange market is centralized, and all data exchanges should be carried out through a trusted third party and some fees should be pay for the services. This way of trading through a third party has some potential safety hazards such as a great possibility of a single point of failure. In order to solve the problem, we can use block chain technology to build a decentralized network instead of the traditional exchange market.

The block chain can make distrust entities reach a consensus and maintain the trust without any third party, because of its decentralization and cannot be tampered with, which can develop a safe and reliable data sharing system. The system is used to ensure the real-time performance of the shared data and also provide protection of transaction privacy. At the same time, for hospitals, banks and other organizations which have a large number of datasets requires special information technology to build a decentralized data exchange system, the block chain can solve this problem effectively.

As shown in Figure 1, in the system users exchange their data through P2P network to solve the problem of privacy security in the process of data exchange, but the problem of small throughput of block chain system will affect the rate of data exchange, frequent network requests cannot be answered immediately. To solve this problem, an information centric architecture is used to optimize information exchange. [5]

In addition, with the increase of data exchange requirements for the IOT, various distributed data exchange platforms have emerged, through which service providers can search and exchange information. However, due to the distrust of these centralized platforms, most users are not willing to put their datasets in them. Therefore, the researchers proposes a decentralized solution of trusted data exchange in IOT based on block chain solution, using block chain and smart contract to achieve a transparent system prototype greatly improves the credibility of data exchange.

3. Conclusion

The block chain technology has brought a dramatic change in IOT network, especially in personal data protection; it can store user's data safely and make it explicitly access to the public data platforms. At the same time, there is no need to trust the third party in data exchange. Although block chain technology has a good advantage in the personal data management, but its lower data transaction throughput is still a problem to be solved. Compared with the central computer management, the transaction processing speed of block chain is still slow, which will seriously affect the transaction performance. Therefore, improving the throughput of block chain will be an important task; it will be one of the directions of the research in the future.

REFERENCES
[1] P. Castillejo, J.-F. Martinez, J. Rodriguez-Molina, and A. Cuerva(2013)Integration of wearable devices in a wireless sensor network for an e-health application, In IEEE Wireless Communications, vol. 20, no. 4, pp. 38–49.
[2] Siwei Miao, Xiao Zhang E-Chain(2020)Block chain-Based Energy Market for Smart Cities, In CENet2020, 1556-1563.
[3] Wang S, Wang X, Zhang Y(2019) A secure cloud storage framework with access control based on block chain, In IEEE Access,7:112713-112725.
[4] Liu T, Wu J, Li J(2019)Secure and balanced scheme for non-local data storage in block chain network, In IEEE 21st International Conference on High Performance Computing and Communications 2424-2427.
[5] Y. Yang, Y. Yang, J. Chen, and M. Liu(2018) Application of block chain in internet of things, In International Conference on Cloud Computing and Security. Springer, pp. 73–82.