Application of Block chain Technology in the Field of Network Security

Zizhou Liu [a], Xiaorong Cheng [b]

North China Electric Power University (Baoding), Baoding 071000, China;

[a]l425173263@163.com, [b]xiaor_cheng@163.com

Abstract

With the development of the Internet, the problem of network security has been paid more and more attention. As a new technology, blockchain technology is different from the traditional network security model and makes up for the traditional network security loopholes. The existing environment of the network has been greatly improved. This paper introduces the technology and characteristics of block chain, expounds the characteristics and advantages of block chain technology, and analyzes the application of block chain in network security through a case.

Keywords

Block chain; Network Security; Application .

1. Introduction

As a new but potential technology, blockchain has been applied to the fields of finance, Internet of things, intelligent manufacturing and so on, which has attracted wide attention of all kinds of institutions at home and abroad. The State Council of China has listed blockchain as one of the strategic cutting-edge science and technology, and the World Economic Forum has also predicted and analyzed the application of blockchain, saying that blockchain will reshape the market infrastructure. Although the research on blockchain is still in its infancy, blockchain technology has shown its potential in the field of network security, and the application of blockchain security direction is analyzed. It is expected to be helpful to the application and development of block chain technology in the future[1].

2. Overview of Block chain Technology and its characteristics

Block chain is widely regarded as a distributed account book maintained by participants. In the typical blockchain system, the information will be stored according to the agreed rules of the participants. In order to prevent the information from being tampered with, the system will take the blocks as the unit, the blocks in chronological order, and form the chain structure in the way of encryption. When the new block is generated, the record node is selected through the consensus mechanism, and the node determines the data of the latest block. Other nodes participate in the verification, storage and maintenance of the latest block data. Once the data is confirmed, it is difficult to delete and change. Only authorized query operations can be performed[2].

The main characteristics of block chain are as follows:

Data can not be tampered with: if data information is saved in the block, all nodes will jointly record the saved information, and through cryptography to ensure the relevance of the information, so the cost of tampering is extremely high.

Anonymity: transactions or exchanges between nodes in a blockchain are based on a fixed, unified rule algorithm, and transactions are address-based and do not need to be traded through personally

identifiable information. Therefore, the two sides of the transaction do not have to guarantee mutual trust, thus ensuring the protection of personal privacy.

Traceability: all historical data is stored on the blockchain system, so each exchange of information on the blockchain can trace the source through the blockchain system.

Information disclosure: the blockchain system ensures the openness and transparency of the information, only a small part of the private information corresponding to each piece of data is encrypted, and the user can view the general ledger and data information on the whole network through any node.

Autonomy: the block chain system is regulated by unified protocol rules, so that each node can exchange data confidently, so the block chain system is not subject to human intervention, which ensures the standardization and stability of the block chain.

3. Application example of Block chain in Network Security

From the characteristics of the above block chain, we can see that in the field of network security, block chain has very obvious technical advantages, and has great application potential in network security.

3.1 Guarantee of data confidentiality and integrity

The network security in the traditional mode is mainly based on encryption technology and trust technology. The data in network communication is easy to be stolen, and the security is difficult to guarantee. The problems of data confidentiality and access control in network communication can be solved by block chain technology. IBM has integrated blockchain networks into their Big Blue cloud services on its Watson IoT platform, and Ericsson's Predix PaaS platform has introduced blockchain technology to ensure data integrity and provide services to the outside world.

3.2 Mitigation of DDoS attacks.

DDoS is a common but effective attack, which uses a large number of requests to occupy network resources, resulting in the paralysis of the target network. The decentralized "accounting" system, owned by blockchain startup Gladius, allows users to rent out their own extra bandwidth and "submit" bandwidth access to blockchain distributed nodes. When the user of the website is attacked by DDoS, the user can mitigate the DDoS attack by renting extra bandwidth.

3.3 Protecting the privacy of social communications

Now that social media has infiltrated our lives, the protection of all kinds of private information has become a difficult problem. Startup Obsidian uses blockchains to protect private communications data for social media chat software. Different from the common end-to-end encryption, Obsidian protects users' metadata through blockchain technology, and metadata is randomly published on blockchain books, which makes it more difficult for attackers to steal information.And can not steal all the information through one node[3]. Not only that, staff of the Advanced Research projects Agency, a division of the U.S. Department of Defense, are also developing an information service that is based on blockchain and is not vulnerable to external attacks.

3.4 Safer DNS

DNS is responsible for mapping domain names to IP addresses on the World wide Web. As the infrastructure of the Internet, it is vulnerable to illegal attacks such as DNS cache infection, information hijacking, redirection and so on. Now many companies are trying to use blockchain technology to avoid security problems. Once the transaction information in the blockchain is confirmed, it is difficult to tamper with it. The Nebulis project based on the blockchain technology uses this feature to record the "increase", "deletion" and "modification" of the corresponding relationship between the domain name and the IP address in the blockchain, and reach a consensus throughout the network[4]. It is difficult to tamper with and form a transaction recording layer to build a more secure and trusted DNS.

3.5 Internet of things

After a long period of development, the Internet of things has provided feasible and effective solutions for intelligent cities, intelligent household appliances and other fields, but it is still faced with some problems, such as the difficulty of establishing network trust system, poor security, difficulty of equipment maintenance and upgrade, and so on. At the same time, considering the high operating cost of data center, Shuling Li et al proposed a lightweight backup architecture based on blockchain. In terms of ride sharing, existing AV/IoT devices usually need trusted third parties, which can lead to trust problems. The CoT framework uses HyperLedger Fabric to build secure and reliable services[5].

4. Conclusion

To sum up, the block chain technology is reliable in network security, which is different from the traditional security technology and makes up for many loopholes in the traditional security technology. Block chain technology still has great potential, but also needs to be continuously expanded and improved. We need to study the block chain technology more deeply, apply the theory to practice, and maintain the security of the network world.

Acknowledgements

Thank my teacher for his careful teaching.

References

[1] Han Xuan, Yuan Yong, Wang Feiyue. Block chain security: research status and prospect [J]. Journal of Automation, 2019, 45 (01): 206 225.
[2] Zhang Qi, Qing Sude, Yang Baixue, Wei Kai, Li Xin. Research on Security risk of Block chain Technology [J]. Information and Communication Technology and Policy, 2019 (01): 46 50.
[3] Yang Hao. A case study of Block chain Application in Network Security [J]. Computers and Networks, 2018, 44 (09): 52 53.
[4] Zhang Tong. Blockchain Technology and Network Security [A]. Professional Committee of Electric Power Informatization of China Society of Electrical Engineering. Digital China Energy Interconnection-Proceedings of 2018 Annual meeting on Informatization of Electric Power Industry [C]. Electric Power Informatization of China Society of Electrical Engineering. Professional Committee: telecom Science editorial Department, people's Post and Telecommunications Publishing House, 2018 / 03.
[5] Song Qianyang, Xu Haishu0069. Key technology and application characteristics of block chain [J]. Network Security Technology and Application, 2019 (04): 18 / 23.