ISSN 2616-5775 Vol. 5, Issue 2: 87-89, DOI: 10.25236/AJCIS.2022.050214

Discussion on Blockchain System Attack and Defense Technology

Guorong Chen

Jiangxi University of Software Professional Technology, Nanchang, China

Abstract: *At this stage, China's research on blockchain is gradually deepening, and the number of patents even far exceeds that of western countries. However, with the continuous development and progress of blockchain technology, the problems in the blockchain system attack and prevention of blockchain become more and more obvious. Based on this background, this paper briefly describes the blockchain system, and puts forward scientific and feasible defense technology strategies for blockchain system attacks from data layer, network layer and application layer, hoping to contribute to the better development of blockchain in China. And it can more actively and effectively promote the improvement of China's blockchain system attack and prevention technology, and more effectively enhance China's overall economic strength, comprehensive national strength and international competitiveness.*

Keywords: *Blockchain; System Attack; Defence Technology*

1. Introduction

As a representative of an emerging industry, blockchain technology has attracted the attention of the state and all sectors of society. However, the multi technology integration mode of blockchain has encountered many security threats because of its complexity and diversity. More and more security problems and attack methods appear in people's vision. In this regard, only by adopting effective defense strategies can we better ensure the security of the blockchain network environment and ensure the development of blockchain technology in a better direction. As a new product, blockchain system appears in our vision, full of countless opportunities and challenges. Firstly, the birth and development of blockchain system has brought a new development space for China's economic and social development. Secondly, the emergence of blockchain has also brought varying degrees of threats to some traditional industries. Therefore, for the development of blockchain system, we should constantly absorb and innovate to effectively promote China's economic development.

2. Overview of Blockchain System

Block chain is a new computer application mode including distributed data storage, point-to-point transmission, and consensus mechanism and encryption algorithm. Its essence is the underlying technology of bitcoin, which coexists harmoniously with bitcoin. In mid-2008, Satoshi Nakamoto published the article Bitcoin: a point-to-point electronic advanced system. It is the publication of this article that marks the birth and application of blockchain system. The publication of this article has also had a certain impact on the development of our society. Although information technology has gradually changed our life in the process of the development and progress of the times, in essence, there are still more traditional ideas in our way of life, and it is difficult to accept this new product for the time being. With the continuous improvement of people's economic level, the understanding of blockchain has also changed to a certain extent, and the blockchain system has begun to receive extensive attention.

The development process of blockchain can be roughly divided into three stages; the first stage is the era of programmable money, which has laid the theoretical foundation for the development of blockchain and formed a perfect technical system, that is, the birth of bitcoin. Bitcoin is simply a digitally encrypted currency. This kind of currency is very different from the physical currency we usually use. It is also circulated through special password encryption. Bitcoin is a currency expression produced by specific algorithms and a large number of calculation methods rather than relying on specific currency institutions. The second stage is the era of programmable application, which improves

ISSN 2616-5775 Vol. 5, Issue 2: 87-89, DOI: 10.25236/AJCIS.2022.050214

the programmability and inclusiveness of the blockchain through new technical algorithms. This technological innovation has laid a practical foundation for the good development of finance, medical treatment, education and other fields. The third stage is the era of programmable society. Blockchain, a new development field, has further promoted the integration and connection between various fields. From mutual integration among industries to mutual cooperation in social fields. With the continuous development of blockchain technology, its functional application of decentralization and de trust has gradually made it surpass more financial fields. The development of the third stage of blockchain is not only extended to the field of social governance, but also includes many fields such as science, culture, industry, literature and art. It has also effectively promoted social development into a new era of intelligent Internet. It can be seen that in the process of continuous innovation, blockchain technology has brought new impetus and new direction to the sustainable and healthy development of China's economy and society.

3. Defense Technology Strategy Against Blockchain System Attack

3.1 The Defence Strategy of Data Layer Attack

The data layer is the lowest layer of the whole blockchain system, which fundamentally determines the security of the blockchain technology network. The data layer ensures that the data of the whole blockchain is not infringed by using a large number of cryptographic technologies. These passwords themselves have certain defects, which brings great challenges and crises to the security of the data layer. Therefore, the data layer may face collision attacks, backdoor attacks, quantum attacks and other threats. In the face of such malicious attacks, we must adopt defense strategies. Due to the defects of its password, it is easy for Internet hackers to deliberately invade. If the password in the data layer is damaged or maliciously stolen by unsettled and kind-hearted people, it is likely to directly affect the long-term and stable development of the blockchain system, and cannot play its own positive role more effectively.

The data layer attacks mainly target the data of the blockchain. From the perspective of privacy, password data protection is the most secure protection mode at this stage. Only by ensuring that the password will not be leaked while designing, can the network security of the blockchain data layer be ensured. However, with the continuous optimization of science and technology, the new generation of computer technology represented by quantum computing is bound to have an impact on the existing cryptographic technology. Therefore, only by switching cryptographic tools at an appropriate time can the security of the overall development of the blockchain be improved. In order to better protect the data layer, defense measures can be taken through three aspects: data confusion, data encryption and covert transmission. Data obfuscation is a privacy data protection mechanism proposed to protect users' privacy in the process of data collection. Data encryption, as its name implies, is a technical measure established and developed on the basis of a password or secret code. When in use, it needs to decrypt and restore the format before it can be used. Covert transmission, as a way of communication, takes special protection measures for the content of transmitted information, so as to achieve the real effect of covert information. At the same time, in order to prevent attackers from maliciously weakening the centralized characteristics of blockchain, we can start with model design to limit the threat posed by malicious viruses. We can start with mechanical learning technology to prevent the virus from being written into the program. [1]

3.2 The Defence Strategy of Network Layer Attack

The network layer is the most basic technical framework of blockchain technology, including networking mode, information dissemination protocol, data verification and other important technologies. At the level of network attack, there may be threats such as client vulnerability, eavesdropping attack, eclipse attack, hijacking attack, segmentation attack, transaction delay attack and so on.

The network layer attacks mainly target the P2P network at the bottom of the blockchain. The purpose of attack is achieved by disturbing the communication mode between users. For information theft attacks, confusing transaction methods can be used to affect the corresponding relationship between unique identification and IP address in the transaction process. The attacker's system identification of user privacy can be confused by sharing location. In addition, in the process of transaction, information disclosure can be prevented by encrypted transmission. For the attack of

ISSN 2616-5775 Vol. 5, Issue 2: 87-89, DOI: 10.25236/AJCIS.2022.050214

hijacking network router, users can automatically detect and mitigate the system in real time, and solve the problem of privacy disclosure in a short time. For attacks that occupy resources maliciously, we only need to constantly improve the reward and punishment system and optimize the network environment.

3.3 The Defence Strategy of Application Layer Attack

The application layer is the main application carrier of blockchain technology and provides solutions to possible problems in various environments. The attack methods at this level can be roughly divided into the attack in mining scenario and the attack in trading scenario. There may be Oday vulnerability attack, network penetration attack and address tampering attack in the mining scenario. Mining attack is to improve its own economic benefits through abnormal mining methods in the mining process of bitcoin system. The attacks in the trading scenario mainly exist in the trading platform and user accounts. Such as weak password attack, library collision attack, fishing attack, man in the middle hijacking attack, dust attack, etc. The main reason for application layer attacks is that programmers release code under extreme pressure and do not have enough time to solve possible security vulnerabilities in the code. Of course, in the process of working, programmers also need to consider whether the language structure can prevent the program from being exposed to implicit attacks. If there are some relatively complex configurations in the application, inexperienced users are likely to inadvertently enable dangerous options, resulting in reduced security performance. Therefore, we must prevent application layer attacks. [2]

Compared with other levels of blockchain, the application layer is more complex. Attackers have a variety of attack methods for this layer. In the development stage, the first is to set the software life cycle, establish a security mechanism to manage vulnerabilities, and test and exploit vulnerabilities before putting into operation. In the deployment stage, the security technology detection of software is added to further prevent the emergence of network security problems. Finally, establish a supervision system of mutual supervision. Ensure the healthy operation of blockchain application layer.

Conclusion

To sum up, the rise and application of new technologies are bound to bring new risks. In order to solve the attack problems existing in the operation of the blockchain system, it is necessary to endow it with a diversified prevention system. With the continuous updating of blockchain technology, it has important scientific research value and good application prospects, and even once rose to one of China's development strategies. In view of the challenges faced by blockchain technology at this stage, it is necessary to make reasonable responses in three aspects: data layer, network layer and application layer, so as to promote the more stable development of science and technology in China.

Acknowledgements

The science and technology research project of Jiangxi Provincial Department of Education: Research on digital copyright protection based on block chain Technology (No. GJJ191491).

Jiangxi educational science "14th five year plan" project: Research on the application of blockchain technology in the process of vocational education modernization -- Taking Jiangxi Software Vocational and Technical University as an example (No. 21YB309).

References

[1] Pang Weibo. Overview of blockchain network security technology [J]. Network Security Technology & Application, 2021(11):21-23.
[2] Li Yu, Duan Yuhong. Survey of crowdsourcing applications in blockchain systems [J]. Computer Science, 2021, 48(11):12-27.