Implementation of Personal Information Security Protection Technology Based on Block Chain

Xu Wei, Leng Jing

Department of Information Technology, Hubei University of Police, Hubei Cooperative Innovation Center for Electronic Data Forensics, Wuhan, Hubei, China, 430034

Keywords: personal information protection; block chain; application

Abstract: The decentralization and intelligence of block chain technology are consistent with the concept of personal information protection. The industry generally believes that its application in personal information protection will effectively support the development of multiple types of personal information systems and the extensive participation of multiple users. This paper analyzes the application of personal information protection to block chain application based on the actual technical requirements and application requirements of personal information protection. Aiming at the problems of information security such as loss of private key and disclosure of privacy, the corresponding countermeasures are proposed. Finally, this paper interprets the application of current block chain in personal information protection.

1. Introduction

At present, with the development of information technology, digitization enters every aspect of life. Regardless of what people do, they may use certain personal information in digital identities, such as entering a password, using a credit card, and issuing a social security card account, or use digital means to sign contracts. It can be imagined that the fragmentation of digital identities is quite serious [1]. The complete personal information identity is closely related to everyone's body, speech, behavior, assets, and reputation, and is therefore a valuable asset. When block chain technology emerges, all organizations can deploy it. This emerging, potential technology and method can establish trust relationships among users, by using collaborative digital books and predetermined block chain individual contributors or manager networks, enabling enterprises to quickly formulate, approve and verify various types of transactions. Once the transaction or other data is recorded in the block chain account, encryption technology and verification settings can greatly reduce the possibility of data being stolen. The system architecture of the block chain is showed in the following figure.

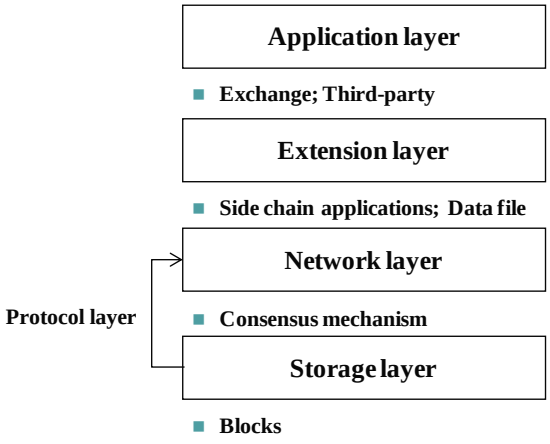

Fig.1 Block chain system architecture

2. The Implementation of Block Chain Encrypted Information System

The participating nodes in the block chain system are all equal. All nodes jointly make decisions and verify the legitimacy of the transactions. Even if some nodes in the system are attacked and destroyed, it will not damage the entire block chain system [2]. At the same time, the block chain guarantees traceability and non-degradability of information through technologies such as encryption mechanisms and digital signatures. An attack model is used to analyze the potential risk of attack on the block chain. The evolution between the honest chain and the attack chain uses the binary tree random walk process. The probability of the attacker successfully eliminating the gap between the established *z* blocks is similar to the gambler bankruptcy problem. Therefore, the probability of the attacker successfully catching up with the honest chain is calculated as follows equation:

$$q_z = \begin{cases} 1, p \le q \\ (\frac{q}{p})^2, p > q \end{cases} \tag{1}$$

Where *p* is honest nodes, *q* is the probability of block bookkeeping rights, with *p+q=1*.

$$q_s = \sum_{k=0}^{\infty} \frac{\gamma^{k_e - \gamma}}{k!} \begin{cases} 1, k > z \\ (\frac{q}{p})^{(z-k)}, k \le z \end{cases} \tag{2}$$

Where q_s is the probability, that attacker successfully tampers. And $\gamma = z\frac{q}{p}$ is the expected value. Based on the above principles, the attacker's tamper success rate is simulated with the relationship between *q* and *z*. The results are shown in the following Figure 2.

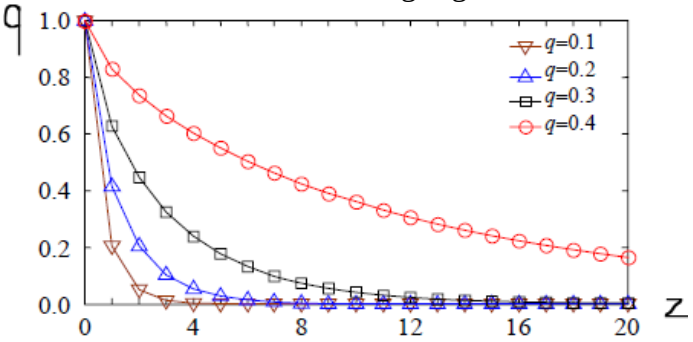

Fig.2 Success rate for attackers

According to figure 2, we can see that the attacker's tamper success rate decreases exponentially as the block gap *z* increases, and when the block gap is fixed, the block pseudo power increases sharply with the attacker's computing power. Therefore, to prevent mutual deception between the various participants, any participant can verify whether the share submitted by a certain participant is valid or not, and no real secret share is required in the reconstruction, which ensures high processing efficiency, without having to maintain a safe passage.错误!未找到引用源。

3. Analysis of the Applicability of Personal Information Protection Block Chain

3.1 Key features of personal information block chain

At present, the block chain has the following features as showed in table 1.

According to the characteristics of the block chain, the block chain and personal information security protection complement each other. The former can provide technical support for the latter and promote the construction of a new type of personal information supply and demand system; the latter can provide the market and application background for the former and achieve technical value. . Compared with the traditional network system, the advantage of block chain is mainly reflected in three aspects: security, transparency and efficiency. Personal information security protection has the characteristics of decentralized supply and demand, flatness of the system, and openness of

transactions, and thus the block chain and personal information security protection have found a point of convergence.

Table1. Block chain features

Features	Description
Distributed storage	Based on P2P networks. Using synchronization algorithm, the block chain data can be completely unified at each node.
Transparent	Each node keeps a backup of data and obtains the latest data in real time. Data can be arbitrarily searched and queried, and is not encrypted.
Security	Before modified, data must be verified, to pass the verification, the entire block chain must be modified, which is the clever use of encryption technology.
Traceability	Each transaction can be traced back from any block, and can be found through the block to find out all the transactions associated with it.

3.2 Applicability analysis

To determine whether the introduction of block chain in personal information security protection is appropriate or not, first, it is necessary to analyze the feasibility of introduction, and the second is to analyze the necessity of introduction. From the analysis of personal information security protection and block chain concept, it is concluded that the two have three common concepts of decentralization, intelligence and sharing. In addition, in the personal information security protection, the personal information security router obtains the energy flow status information through the information flow, thereby realizing functions such as scheduling and control. In the future, the functions of block chain nodes can be realized by installing distributed computing and data storage modules on personal information security protection routers and loading specific smart contract procedures [3]. In summary, it is feasible to introduce block chain in the protection of personal information security, both conceptually and technically.

4. The Security Challenges and Countermeasures of Personal Information Security Protection Based on Block Chain

4.1 Lost private key

The information on the block chain cannot be modified, but it is premised on the security of the private key. The commonly used private key storage scheme is that each user in the block chain system encrypts the private key and stores it on the user's device. However, this method cannot resist the attacker's use of an offline dictionary attack after acquiring the user's device. So block chain faces the risk of stealing private keys. In order to prevent the loss of the private key, a secret sharing mechanism can be used to protect the node private key. In the process of secret sharing, each participant uses its identity to identify its own private key share and uses its own private key as a secret share. It can distribute secret shares at the same time as it distributes secretly without any prior processing.

4.2 Privacy leak

Currently, the transaction data transmitted and stored on the block chain are all open and transparent, and certain privacy protections are provided for the identity information of the transaction parties by separating the pseudo-anonymity of the transaction address from the real identity of the address holder. However, the correlation between the account and the transaction can still be found through the information. For the Internet, which involves a lot of personal information privacy, the disclosure of data clearly does not meet regulatory requirements. In particular, sensitive data needs to balance privacy protection and compliance supervision. On the one hand, it is necessary

to protect the privacy of transactions of participating parties on the block chain. On the other hand, it is necessary to prevent illegal participants from using it to conduct illegal transactions.

5. Application of Personal Information Security Protection Based on Block Chain Technology

5.1 Prevent data tampering of proprietary networks

One of the main features of block chain is its non tamperability. Although the block chain system is open, the data exchange processes such as verification and transmission use sequential hashing and hashing algorithms, combined with a decentralized structure, it is almost impossible for either party to unilaterally change the data in the block [4]. This technology not only ensures the correct source of data, but also ensures that data is not intercepted in the middle process. Therefore, the block chain is very suitable for organizations that use and process sensitive information, to ensure the integrity of the personal informationd, and prevent any form of tampering, reducing the security risk of traditional networks and the probability of hacking attacks. If the block chain technology is used in the future public security information system for the input and release of data, it is impossible for unauthorized data to be tampered, forged or deleted, so as to ensure the privacy, integrity and security of personal information.

5.2 Prevent distributed denial of service attacks

Block chain technology provides a decentralized fully distributed service solution. Instead of relying on a limited number of servers, it can provide services through the data transmission service between various nodes in the block chain network to implement domain name query and resolution. Therefore, as long as there are still nodes in the network running block chain service system. The corresponding domain name can be accessed, and no one can control it. If you want to attack a large number of distributed block chain servers in the entire network, attackers need a larger number of attack resources that can be invoked, which is also very difficult or even more costly for an attacker.

6. Summary

This article applies block chain technology innovatively to solve personal information protection issues. Based on the current technical requirements and the first application requirements for personal information protection, the feasibility of the application of block chain technology is explained. From the aspects of the technical characteristics of the block chain, the security challenges and solutions, the details of personal information protection based on block chain are analyzed in detail, and the further application of block chain in personal information protection is explained, which further proof of the application of block chain in the field of personal information protection.

References

[1] Liu Yahui, Zhang Tieyong, Xiaolong. Personal Privacy Protection in the Age of Big Data[J]. Computer Research and Development, 2015, 52(1), p.229

[2] Cao Wangxi, Yan Bing. Application Overview of Block chain Technology in Service Field [J]. Power Technology, 2017, 41(3), p.736

[3] SHULTZ B L. Certification of witness: mitigating block chain fork attacks [D]. New York: Columbia University, 2015, p.24

[4] Wang Anping, Fan Jingang, Guo Yanlai. Block chain application in the Internet[J]. Power Information and Communication Technology, 2016, 14(9), p.6