Personal Privacy Protection Scheme Based on Blockchain Technology

Liang Cai, Jianping Chen*, Tao Xu, Wanzhi Wen
School of Computer Science and Technology
Nantong University
Nantong, Jiangsu, China, 226019
*chen.jp@ntu.edu.cn

***Abstract*—In order to solve the problem of frequent leakage of personal privacy information, this paper proposes a personal privacy protection scheme based on blockchain technology. Targeting at the existing problems and combining the advantages of decentralization, trust removal and data unchangeable of blockchains, a framework model is proposed. The objects of the model are designed and explained, and the hash function in blockchain cryptography is used to encrypt and decrypt personal information. The specific processes including uploading information, obtaining user's personal information, reading access record and revoking permission are described. The feasibility test and performance analysis of the scheme are carried out. It is shown that the proposed blockchain based scheme can meet the needs of personal privacy protection and enable users to have strong control over their private information, and it can effectively avoid common network attacks.**

Keywords—blockchain, privacy protection, decentralization, hash function, consensus mechanism

I. INTRODUCTION

With the popularization of information technology and the Internet, a large amount of personal privacy information data is collected and used. It brings great convenience to the production, operation and management of government departments, enterprises and institutions as well as the people's work and life. At the same time, the leakage of personal privacy information has become a serious problem and need to be solved. Traditional privacy protection technologies are mostly centralized architectures. Once the central node is attacked, the entire system will be paralyzed. The blockchain has the characteristics of decentralization and can be used to solve the problem of personal privacy leakage.

The blockchain technology first appeared in "Bitcoin: a peer-to-peer electronic cash system" [1] published by Nakamoto. It introduces the characteristics of blockchain technology, such as decentralization, point-to-point transmission, and consensus mechanism. It can be used as a solution for personal privacy protection. At present, there are a few research papers published in this area. Among them, Swan [8] proposed a mechanism to protect personal data from leakage by blockchain technology, but did not give specific technical details and usage environment. Huang Xiaoju et al. [9] proposed an information management scheme based on blockchain ethereum technology, and gave certain application scenarios, but lacked technical details.

In this paper, we propose a personal privacy protection scheme based on blockchain. Through blockchain technology, a distributed and multi-center privacy protection mechanism is built to provide safe and reliable storage, uploading, verification and other services for personal privacy information. It can also ensure that personal data will not be tampered with or get lost.

II. MODEL AND BLOCKCHAIN DESIGN

A. Model Design

In the process of using personal privacy information, users and third parties' operations on private information are recorded as transaction data in the blockchain, so that the security problem of the traditional centralized mode can be effectively curbed. The general diagram of the scheme is shown in Figure 1.

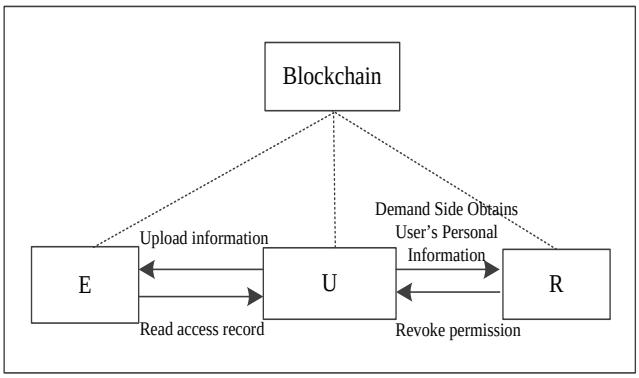

Figure 1. General diagram of personal privacy protection scheme based on blockchain

Participants include the following parties: individual users (represented by U in this paper), which have personally privileged information that needs to be provided to the demanding party; data management platform (represented by S); third-party database (represented by E); and demand side (represented by R).

B. Blockchain Design

Many transactions are involved in the blockchain, and the results of the transaction need to be verified for existence and integrity through the Merkle tree. In the scheme of this paper, the interaction data of different transaction objects is hashed to generate a new hash value. The new hash value is recorded in the blockchain, and then it is recursively operated.

Blockchain trading is the transaction data in the blockchain ledger. In the proposed scheme, different trading objects send transactions on the blockchain to obtain the audit of the transaction content. Figure 2 gives a transaction data structure that conforms to the requirements of this solution in which data is constructed in a specific manner.

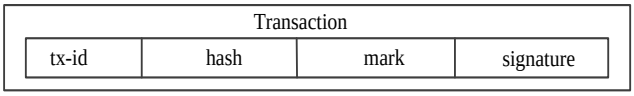

Figure 2. Transaction data structure

In Figure 2, tx-id represents the transaction number of the transaction, hash represents the hash value of a message, mark represents the authorization operation used to record the transaction process, and signature indicates that the user information is encrypted and signed by the private key. The user decrypts the signature using the user address (hash public key).

The blockchain is actually a distributed database with decentralized features with highly decentralized decision-making power. The current main consensus mechanism is divided into proof of work （PoW） and proof of stake (PoS). This paper uses an improved workload proof mechanism to solve the consensus problem. The rules are as follows:

Only one person can record successfully for a period of time; obtain unique billing rights by resolving cryptographic issues; the other nodes on the chain replicate the results of the record.

III. Implementation Procedures

A. Upload Personal Information

The flow chart for uploading personal information is shown in Figure 3.

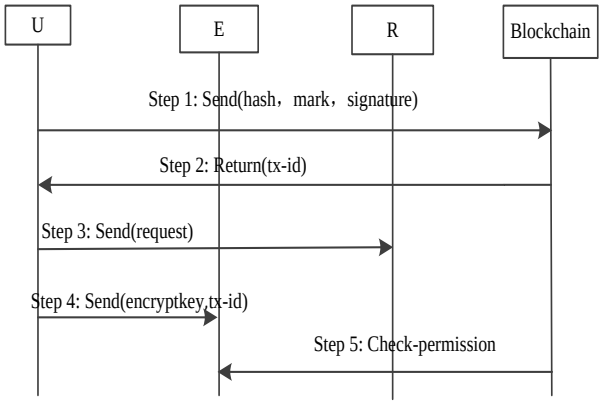

Figure 3. Uploading personal information

The specific process is presented.

Step 1: When the user generates a hash value, the mark operation is performed, and the mark value at this time marks the position of the operation. The blockchain operation authority is granted by the user, the private key is digitally signed to form a signature, and the personal privacy information is sent to the blockchain.

Step 2: Return the transaction number tx-id for this transaction.

Step 3: The client sends a demand request command to the demand side.

Step 4: The user provides personal privacy information and uploads it to the database, and simultaneously sends the public key and tx-id.

Step 5: The blockchain queries the personal privacy information which is sent to the database, and performs the query operation through the transaction number tx-id. After the consensus mechanism, the traversal is sequentially performed for extraction. Decryption needs to use the private key to read the corresponding operation to get the specific content. At this point, the decrypted mark and signature are verified. After the completion of the database, the database will store the extracted mark and signature information.

B. Demand Side Obtains User's Personal Information

The flow chart of the demand side to obtain the user's personal information is shown in Figure 4.

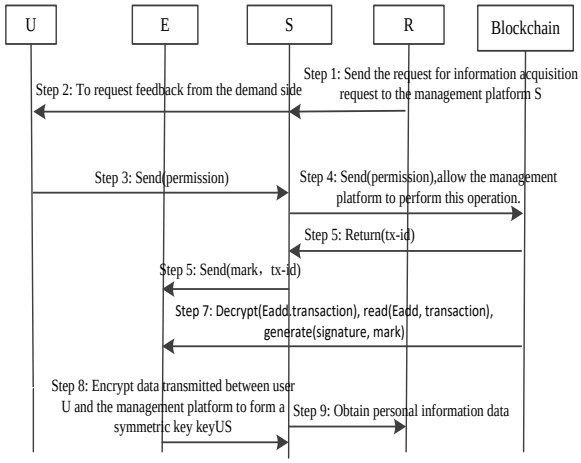

Figure 4. The demand side obtains the user's personal information

The specific process is given.

Step 1: The demander must first send a request to the management platform to obtain the user's personal information.

Step 2: After receiving the request, the management platform will feed it back to the user and ask for user consent.

Step 3: The client receives the feedback from the management platform and sends the permission to the management office, and allows it to perform the operation.

Step 4: The blockchain traverses the transaction number tx-id to extract the corresponding data, and then decrypts it. The user uses the private key to read the corresponding operation, obtains the specific content, and verifies the decrypted mark and signature. After the completion of the database, the database will extract the information such as mark and signature.

Step 5: Return the transaction number tx-id for this transaction.

Step 6: The management platform sends the mark, transaction number tx-id to the database.

Step 7: The blockchain uses the private key to read the corresponding operation and obtain the specific content. Then it will verify the decrypted mark and signature. After the verification is completed, the database is extracted and stored.

Step 8: Encrypt the data which is passed between the user and the management platform to generate keyUS.

Step 9: The demand side obtains the user's personal information data.

C. User Read Access Record

The flow chart for the user to read the access record is shown in Figure 5.

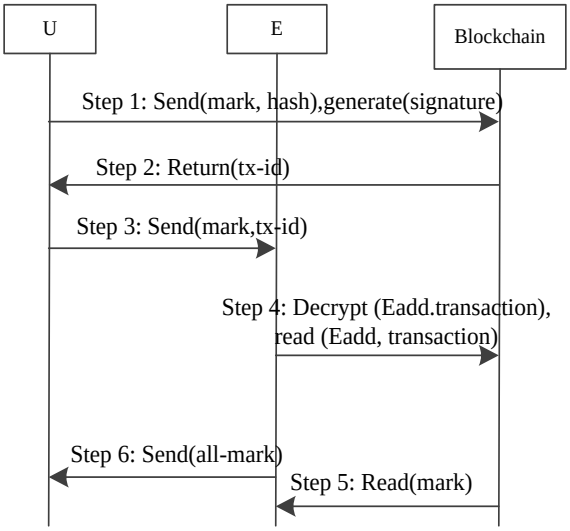

Figure 5. User read access record

The specific process is described.

Step 1: The client sends the mark value to the blockchain. The mark value records the visitor record. it contains the user's authorization record and generates a digital signature.

Step 2: Return the transaction number tx-id for this transaction.

Step 3: The client sends the mark value and the transaction number tx-id to the database.

Step 4: After receiving the signature information signed by the database, the block link decrypts through the blockchain address Eadd and also its private key.

Step 5: The blockchain reads all the operations performed by the database.

Step 6: The database sends all the operations performed by the demanding party to the client, and the user can see all the visitor records and all the operations.

D. Revoke Permission

The flow chart for revoking permissions is shown in Figure 6.

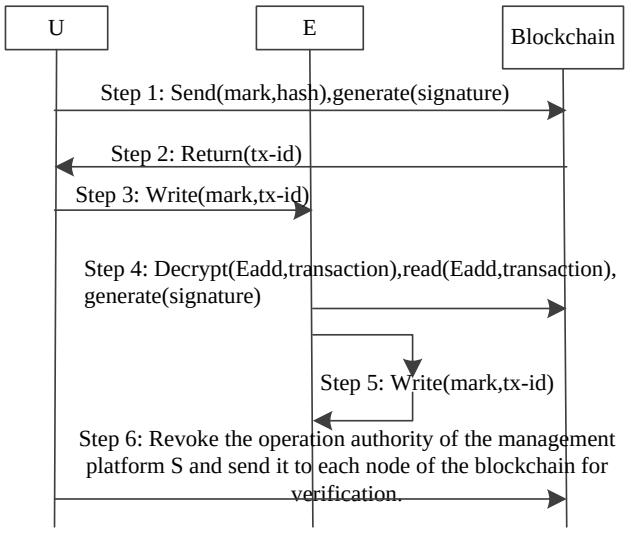

Figure 6. Revoke permissions

The specific process is provided.

Step 1: The client sends the mark and hash values to the blockchain and generate a digital signature.

Step 2: Return the transaction number tx-id for this operation.

Step 3: The client sends the transaction number tx-id to the third party database.

Step 4: The blockchain uses the private key to decrypt the transaction sent by the database, and stores the extracted information to complete the verification of the digital signature.

Step 5: The database verifies the transaction number tx-id sent by the client.

Step 6: The user revokes the operation authority of the management platform through the blockchain and sends it to each node of the blockchain for verification.

IV. Performance Analysis

A. Replay attack

In the scheme, the random number is added at the same time as the message is transmitted. The random number is stored in the third-party database. Before the feedback information is verified, the random number is first verified, and the random number is verified to be the same as the original one to prevent the replay attack.

B. Man-in-the-middle attack

The personal privacy information is first hashed to obtain a hash sequence, which is broadcasted to the entire blockchain network through a secure channel to ensure that the authentication information is not tampered. When different nodes in the blockchain network communicate, the related information such as Uadd and UID is transmitted through the secure channel, and the malicious third party cannot tamper with it, which can effectively prevent the man-in-the-middle attack.

C. Camouflage attack

In the blockchain, the transaction activities among any nodes are supervised by the entire blockchain network, and

the database adopts distributed storage. It is impossible for a malicious third party to pretend to illegally obtain the privacy information of the individual user. Therefore, the proposed scheme can effectively prevent camouflage attacks.

D. Resist Distributed Denial of Service (DDoS) attack

For the traditional centralized privacy protection mechanism, once a node has problems, the entire system will not work properly. With the proposed blockchain based solution, the fail of any single node does not affect the normal operation of other nodes. There is no such problem of single point failure. It is more flexible than a traditional centralized system in terms of denial of service attacks. For the latter, once a node fails, users which are connected to the failed node cannot enter the system.

V. CONCLUSIONS

In the centralized architecture of traditional privacy protection, if the central node fails or is attacked, the entire network will be paralyzed, and the user's personal privacy information may be leaked. This paper proposes a blockchain based personal privacy protection scheme. It encrypts the user's personal important information through a hash function, and uses the workload proof mechanism to record the user's transaction information data in the blockchain's ledger and cannot be changed. Using this scenario, once a user has registered personal information in a third-party platform, the platform cannot sell its personal privacy information to others without authorization from the user. The user can view all access records through the management platform or cancel authorization at any time. The scheme proposed in this paper is versatile and can be applied to some software platforms that integrate huge personal information data such as the platforms of shared bicycles and digital payments.

ACKNOWLEDGEMENT

This research work was financially supported by the National Natural Science Foundation of China (grant No. 61602267).

REFERENCES

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electroic cash system [EB/OL]. http://bitcoin.org/bitcoin. pdf.

[2] Zhu Lihuang, Gao Feng, Shen Meng, Li Yandong, Zheng Baokun, Mao Hongliang, Wu Zhen. Summary of Research on Blockchain Privacy Protection[J]. Journal of Computer Research and Development, 2017,54(10):2170-2186.

[3] Banisar D, Davies S. Global trends in privacy protection: An international survery of privacy, data protection, and syrveillance laws and developments[J]. Journal of Computer & Information Law, 1999, 18(1): 3-111..

[4] Smith H J, Milberg S J, Burke S J. Information privacy: measuring individuals' concerns about organizational practices [J]. MIS Quarterly, 1996, 20(2): 167-196.

[5] Bertino E, Sandhu R. Database security-concepts, approaches, and challenges[J]. IEEE Trans on Dependable and Secyre Computing, 2005, 2(1): 2-19.

[6] Liu Yahui, Zhang Tieying, Pei Xiaolong, Cheng Xueqi. Personal Privacy Protection in the Age of Big Data[J]. Computer Research and Development, 2015, 52(01): 229-247.

[7] Fang Xingshu. Key Technology Implementation of Trusted Degree Inquiry System Based on Blockchain[D]. Dalian Maritime University, 2017.

[8] SWAN M. Block chain thinking: the brain as a decentralized autonomous corporation [commentary][J]. IEEE Technology & Society Magazine, 2015, 34(4): 41-52.

[9] Huang Xiaoju, Xu Wenqi, Zhang Tao, Gong Xueqing. Personal Information Management Based on Blockchain Technology[J]. Software Engineering, 2018,21(10):34-37+30.

[10] Yuan Yong, Wang Fei-yue. Blockchain: the State of the Art and Future Trends[J]. Acta Automatica Sinica, 2016, 42(04): 481-494.G.

[11] Hovland G, Kucera J. Nonlinear feedback control and stability analysis of a Proof of Work Block chain Modeling Identificationand Control, 2017,38(4):157-168.

[12] Franco P. Understanding Bitcoin: Cryptography, Engineering and Economics [M]. Hoboken:Joho Wiley & Sons,2014.

[13] Dong Guishan, Chen Yuxiang, Zhang Zhaolei, Bai Jian, Hao Wei. Research on Identity Management Basedon Blockchai Identity Management[J]. Computer Science, 2018(11):52-59.

[14] Das M L, Saxena A, Gulati V P. A dynamic ID-based remote user authentication scheme[J]. IEEE Transactions on Consumer Electronics, 2004, 50(2):629-631.

[15] Wang Y Y, Liu J Y, Xiao F X, et al. A more efficient and secure dynamic ID-based remote user authentication scheme[J]. Computer Communications, 2009, 32(4):583-585.

[16] Xiong L Junguo L Jiao Zet al. A secure remote user mutual authentication scheme using smart cards[J]. IEEE Computers, Communication sand IT Applications Conference, 2014,89-92.