Research on Cross-chain Technology Architecture System Based on Blockchain

Jianbiao, Zhang [1] and Yanhui, Liu [1]

[1] Beijing University of Technology, Beijing 100124, China

Abstract. With the development of blockchain technology, blockchain technology has strong vitality in various industries due to its characteristics of dispersion, anti-mite modification and traceability. Blockchain technology allows trusted parties to trust transactions and realize value streams. Since there are different values in different chains, will the values of different chains also flow? This is a problem that needs to be solved in the cross-chain interaction. Under the scenario for cross-chain interaction between private chain or alliance chain between enterprises, this paper proposes an alliance chain model that can realize cross-chain interaction between enterprises. On this basis, it analyzes the difficulties of cross-chain interaction technology and analyzes the model. At last, we summarize the paper.

Keywords: block chain, cross-chain interaction, authentication, zero knowledge proof, privacy protection, alliance chain, data sharing

1 Background

In recent years, with the rise of digital cryptocurrencies such as Bitcoin, blockchain technology has attracted widespread attention in various industries. In essence, blockchain technology is a technical solution for collectively maintaining a reliable database through decentralization and high trust. [1] Its core technologies include distributed ledger technology, asymmetric encryption algorithms, and smart contracts, etc. It also has the characteristics of decentralized consensus mechanisms, traceability, and high levels of trust. At present, with the development of blockchain technology, it has developed three eras. The first era is bitcoin era, the second is smart contract era and the current blockchain 3.0 era. In the current era, blockchain technology is no longer limited to finance area. It extends to any area which involving multiple trust needs, such as auditing, notarization, medical care, voting, logistics, etc. It is also influencing the entire society. The inherent advantages of blockchain technology that other technologies do not have enable it to change the existing operation mode, change production mode and improve production efficiency in many industries [2].

With the rapid development of blockchain technology, various types of blockchains have sprung up. Blockchain becomes a very good value carrier due to its decentralization and tamper-proof characteristics. Each blockchain is a carrier of value. Based on actual business scenarios, there is a need to achieve value transfer on different chains, or information exchange between chains. These scenarios are collectively referred to as cross-chain interactions. In the cross-chain process, it is necessary to

study appropriate methods and techniques to realize the privacy protection of interactive information.

With the application of blockchain technology in various industries, different companies or organizations may establish their own blockchain according to business needs, and different block chain structure will be different. Regardless of the structure of the blockchain, one blockchain cannot actively recognize the external chain. This makes the data or value in the blockchain unable to transfer directly between different blockchains, and this thing is actively or passively leading to value islands. Therefore, the problem of cross-chain interaction has become an inevitable trend in the research of blockchain. At the same time, the security problems arising in the process of cross-chain interaction are worthy of further study. Due to the distributed nature of the blockchain, for each single chain, the information on the chain is open to all nodes on the chain, but for other chains some of the information may need to be protected. In the cross-chain process, how to effectively protect the private information of the blockchain participating in the interaction, how to ensure the identity authentication of other blockchains in the cross-chain process [3-5] and the sharing of related public information are the core issues which needs to be solved.

Although blockchain has the characteristics of decentralization, non-tampering and traceability, there are various attack methods against blockchain technology, such as solar eclipse attack [6], selfish mining attack [7-8], reduce block attack [9-10], bribery attack [11], double expense attack, DDOS attack, etc. Under single-chain conditions, data security and privacy are seriously threatened, and the security issues faced in cross-chain interactions are even more severe. Under the conditions of the current blockchain application scenario, beyond the financial field, jumping out of the inherent circle of digital currency and value transfer [12], thinking about the interaction and sharing of data between chains, and how to interact between chains, how to realizing the protection of private data has become an urgent problem we need to solve now. Considering the rapid development of blockchain technology, it is of great significance to study the privacy protection problem under cross-chain interaction conditions.

At present, scholars from various countries have conducted extensive research on the privacy protection of blockchain. Herrera-Joancomarti [13] made a detailed review and summary of the anonymity of Bitcoin. The literature believes that most researchers regard blockchain technology as a natural role for privacy protection. Only a few documents consider that bitcoin transactions may reveal private information. Although the blockchain can achieve privacy protection, it is pseudo-anonymous, which means there are still possible links between different transactions and addresses. Spagnuolo et al. [14], Herrera et al. [15] and Moser et al. [16] all pointed out we can find the relations between the address and the user from multiple input addresses based on the same transaction which belong to the same user.In addition, some research on security attacks has revealed privacy threats to blockchains. Feld et al. [17] and Koshy et al. [18] proposed a method for associating bitcoin addresses with IP addresses from the perspective of analyzing network traffic. Moser et al. [16] and Bahack [10] use a centralized server to track multiple addresses of the same user or the true identity of the user. So the user's address is at risk of anonymity.

Meiklejohn et al. [19] collected the bitcoin addresses published on the Bitcoin forum and then used the stain analysis and clustering methods to find the identity information of many bitcoin addresses. Huang et al. [20] proposed a malicious node detection method based on behavior pattern clustering, which can quickly locate malicious nodes and eliminate the hidden dangers of privacy leakage caused by malicious nodes.

In addition to researches on the privacy protection of blockchain, different blockchain attack methods are also a hot research topic. For example, Zhu Lihuang et al. [21] introduced the blockchain technology architecture and defined the concepts of identity privacy and transaction privacy in blockchain technology, and analyzed the advantages and disadvantages of blockchain technology in privacy protection. In the research, he stated the blockchain privacy attack method and then forecasted. Li Kang et al. [22] also discuss privacy protection issues. The literature summarizes the existing privacy protection schemes, focusing on zero-knowledge proof technology. The paper explains and analyzes the technical challenges of applying zero-knowledge proof to the blockchain privacy protection scheme, and gives a guiding solution, but how to ensure effective protection of the already-chained information in the cross-chain interaction process has not received much attention.

The issue of privacy protection is very important, and it is one of the key issues for the application of blockchain technology [23]. However, there are few studies on cross-chain interactive security issues. In the study of cross-chain, Maurice Herlihy et al. [24] proposed the exchange of atomic cross-chain assets, such as trading bitcoin as ethereum and giving atomic exchange protocol; Wang Hui et al [25] proposed a cross-chain communication protocol, giving a communication solution for blockchain routers which enables different blockchains to communicate with each other like the Internet. At present, for the cross-chain technology is still in research and experiment, some well-known technologies include the notary mechanism, side chain, hash lock and other technologies. There are currently corresponding solutions for different cross-chain technologies. For example, Ripple Labs proposed notary public mechanism and Interledger protocol in 2012, aiming to connect different accounts and achieving synergy between them, enabling two different accounting systems. Freely transfer money to each other through third-party "connectors" or "verifiers", as long as the two parties reach a consensus, they can trade without mutual trust. For sidechain technology, Blockstream has developed an element chain project, as shown in Figure 1. Two-way peg allows Bitcoin to interchange between the main chain and the side chain, while also bringing many innovative technologies to Bitcoin including private transactions, evidence separation, relative lock time, and new opcodes, signature coverage amount and other characteristics, these technologies can be applied to any sidechain with any combination; for hash lock, the original intention is to hope that chain A and chain B know each other as little as possible, and as a way to eliminate the trust of notaries. Means, the basic process of the model is shown in Figure 2. The representative projects include the aforementioned interledger, lightning network and so on. However, the existing cross-chain projects are more focused on digital currencies such as bitcoin, and do not pay enough attention to the privacy protection issues generated in the cross-chain process and do not have specific solutions.

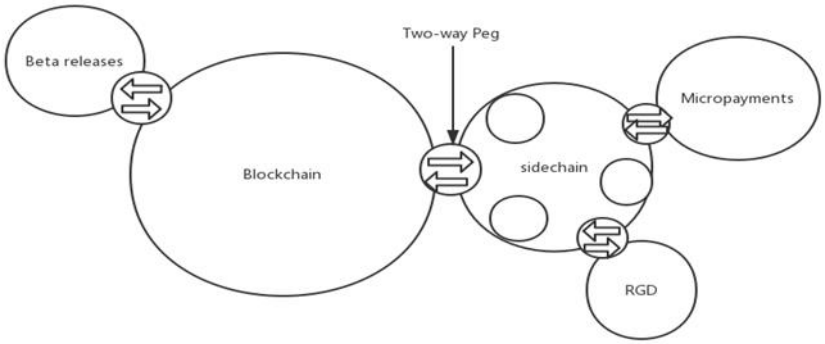

Fig. 1.Side-chain technology

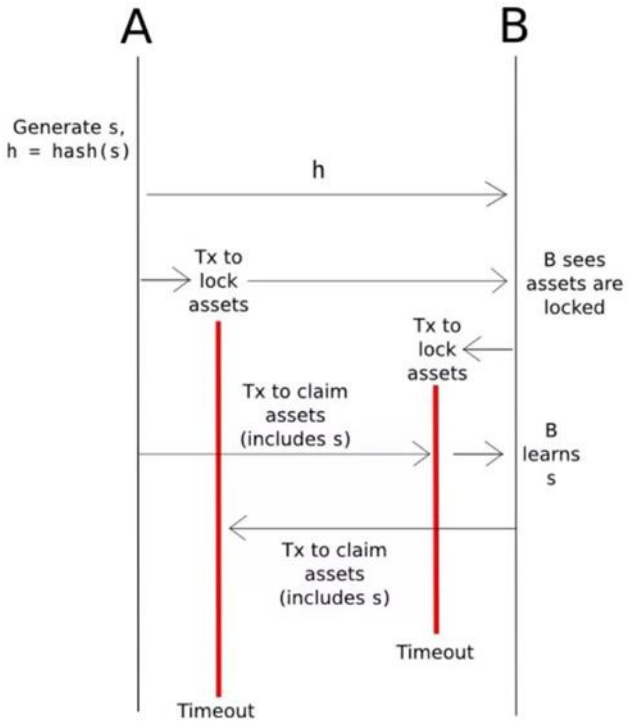

Fig.2. Hash lock technology

It is an inevitable trend for blockchain to be interconnected, which also meets the needs of social integration and development. At present, the blockchain technology is in the initial stage, and the focus is on the combination of blockchain and practical application scenarios. Most of the research is still in the background of single chain, and the research on cross-chain technology is just starting. Accordingly, to blockchain privacy problem, although many institutions and scholars have recognized this, but

there is no in-depth study. Therefore, to carry out the cross-chain privacy protection problems has very important practical significance.

2 Difficulties in cross-chain

The difficulty of cross - chain technology lies in the following aspects:
1. How to verify the state on the original chain in a distributed way. As the information between chains cannot interact directly with each other, blockchain is also a state machine model in nature. On the blockchain, every transaction packaged or new block generated will change the state of the whole blockchain. The transaction information on the original chain is external information for another chain. How to ensure that this external information is correct when entering another chain is the important link of the whole cross chain mechanism. In addition, in the case of centralized nodes, information of chain A can be cross-linked to chain B. It is much easier to confirm whether this process is completed or not. However, in the case of decentralized distribution, it is difficult to confirm whether the cross-linked transaction of user A on chain A is completed.
2. How to ensure that the total number of tokens on the original chain remains unchanged after cross-chain interaction. After each cross-chain interaction, the total number of tokens on the original chain can neither increase nor decrease, but only enter the locking state. At the same time, the token locked before can be unlocked after the same pen value crosses the original chain. As the general chain does not have the function of realizing cross-chain, it is necessary to design a reasonable method to extend the block chain structure and operation mechanism involved in cross-chain reasonably. Furthermore, since the blockchain includes public chain, alliance chain and private chain, it is necessary to design a reasonable extension scheme to support cross-chain.
3. How to guarantee the atomicity of cross-chain transactions. In the process of crossing the chain, it is necessary to guarantee that the cross chain transaction either ends completely or can be revoked, that is, if one link of the cross chain is terminated for various reasons, the whole cross chain transaction should be revoked, otherwise it will result in double payment.

3 Architecture and Analysis of cross-chain

This thesis focuses on the scenario of cross-chain interaction between inter-firm alliance chains and private chains. The cross-chain interaction process and information designed by the project can be managed and maintained by an industry association or an alliance chain maintained by the industry chain alliance. The project is collectively referred to as the interactive alliance chain. According to this scenario, the paper designed a cross-chain interaction architecture model to solve the problems of identity authentication, privacy protection, data security sharing in the cross-chain interaction process.

In order to avoid the user identity forgery involved in the cross-chain, which leads to the disclosure of user information in another chain, PKI technology is adopted to verify the identity information involved in the cross-chain. There are two cases, one is PKI technology has already been used in the chains, and the certificate will be attached when the cross-chain request is submitted. The other is PKI technology is not used and the participants need to apply for certificates of identity for authentication before across chain.

For a cross-chain interaction, the two or more parties involved in the cross-chain may only interact with the service for a certain demand, such as participating in the auction of a luxury or large-value product. The identity of the buyer's enterprise may not want to be leaked to the seller or other parties, in which case the buyer only needs to provide the seller with the necessary valid information, such as the buyer's qualification of product or raw materials purchase. And the seller can verify the transaction, which involves zero-knowledge proof technology. In this way, the privacy of the cross-chain interaction related parties can be protected to the utmost extent.

In cross-chain interaction, it must involve the interaction of data. These data may be sensitive data inside the enterprise. These sensitive data may only be accessed or used by other specific enterprise customers within a limited time, so the cross-chain interaction process involves the issue that how data is shared securely, such as cross-chain (or cross-domain) dynamic access control. Since smart contracts naturally have the advantage of trust and intelligent execution, the relevant conditions in cross-chain interaction can be transformed into smart contracts. Some of the qualifications in these conditions can include roles, destination addresses, decryption keys, granular access rights, effective time limits, and so on. The smart contract can sign and deploy the smart contract to the interactive alliance chain after the two or more parties reaching the agreed condition, waiting for the smart contract to be automatically executed under the condition that the condition is satisfied, and realize the safe automatic and efficient execution of the data sharing. The overall architecture model of cross-chain interaction is shown in Figure 3.

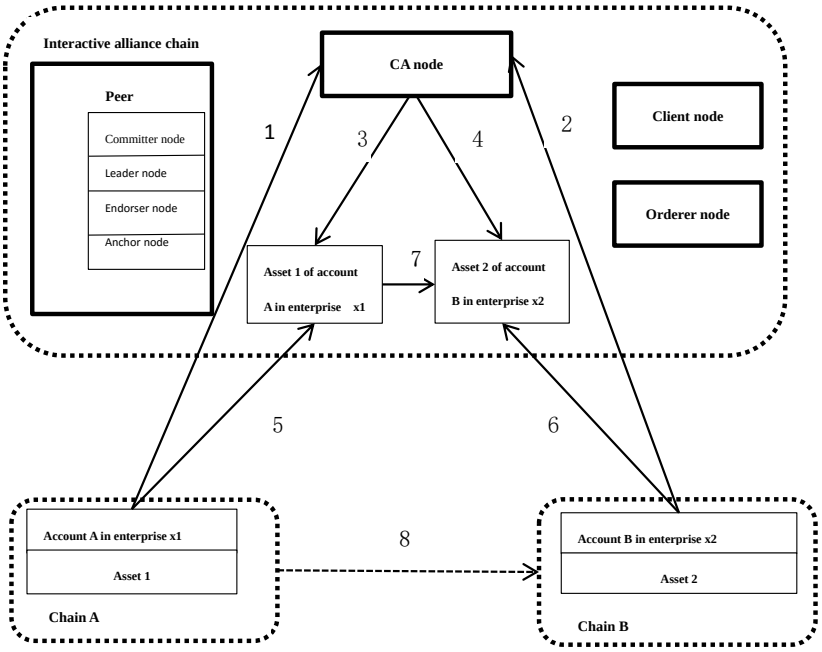

Fig. 3. The architecture for cross-chain interaction

In this architecture, the process of cross-chaining is described as follows:

1. The enterprise A user of the A-chain uses the certificate carried by itself (published by the A-chain CA) or applies for a certificate through the CA node of the interactive alliance chain;

2. The enterprise B user of the B-chain uses the certificate carried by itself (published by the B-chain CA) or first applies for a certificate through the CA node of the interactive alliance chain;

3. After the certificate is verified by the CA node in the interactive alliance chain, a new enterprise A account is allowed to be created on the interactive alliance chain.

4. After the certificate is verified by the CA node in the interactive alliance chain, a new enterprise B account is allowed to be created on the interactive alliance chain.5. Enterprise A of the A-chain initiates a cross-chain request. The request is to exchange the assets of the enterprise B user on the B-chain with the asset 1 on the chain. The interactive alliance chain confirms the enterprise user A by calling the query interface of the A-chain. Asset 1, then add the encrypted asset 1 to the enterprise A account on the interactive alliance chain, and freeze the asset 1 of the enterprise A account on the A-chain;

6. The interactive alliance chain confirms that the enterprise user B owns the asset 2 by calling the query interface of the B-chain, and then adds the encrypted asset 1 to the enterprise A account on the interactive alliance chain, and freezes the asset 2 of the enterprise B account on the B-chain;

7. The interactive alliance chain generates a mapping of the encrypted asset 2 of the enterprise B account to the encrypted asset 1 of the enterprise A;

8. Finally, through the cross-chain interaction process, the value flow of asset 1 from A-chain to B-chain and value flow of asset 2 from B-chain to A-chain are gained.

In addition, if Enterprise A wants to exchange assets 1 through a cross-chain approach again, it will be found in the interactive alliance chain that the asset has been transferred, which means Enterprise A has no ownership of the asset. Then the interactive alliance chain will reject the cross-chain request.

The cross-chain model belongs to the alliance chain type, and the P2P network is responsible for the underlying network node discovery, node data synchronization, etc., which includes the block, the account book, the consensus mechanism, the intelligent contract module, and the responsible authority management and PKI system, as shown in FIG. 4. All cross-chain interactions related information, such as identity authentication, negotiation, smart contracts, data sharing, will be saved to the alliance chain. The coalition chain also contains super nodes, which can review all cross-chain interaction information.

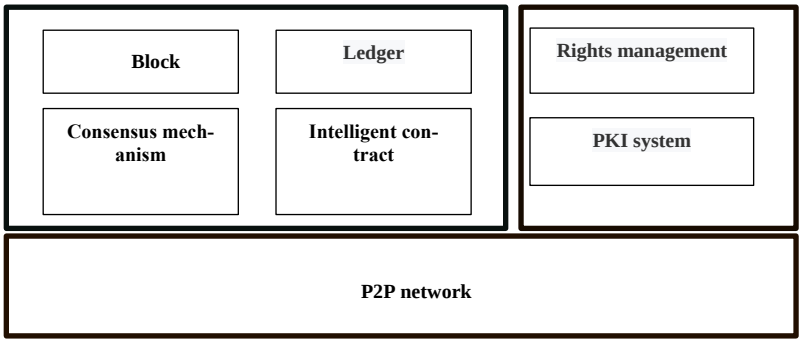

Fig. 4. Cross-chain interaction alliance chain model

4 Conclusion

Cross-chain interaction is a requirement that blockchain technology will inevitably appear after large-scale application. With the researching on the current research status of cross-chain interaction, this paper analyzes the difficulties of cross-chain interaction technology, and then targets the alliance between enterprises scenario, especially in cross-chain interaction between alliance chain or private chain. The architecture of cross-chain is also proposed. Finally, cross the chain interaction is block chain technology in large scale after one of the inevitable demand, this paper introduces the existing cross-chain researches, then analyzes the technical difficulties of cross=chain interaction. Targeting to league chain and private chain, this paper proposes a cross-chain architecture, and cross-chain interaction process is also analyzed.

References

1. Nakamoto S. Bitcoin:A peer-to-peer electronic cash system[EB/OL]. [2017-08-01].http://www.bitcoin.org/bitcoin.pdf.
2. Swan M. Blockchain: Blueprint for a New Economy [M], Blockchain: blueprint for a new economy. O'Reilly, 2015.
3. Fromknecht C,Velicanu D.CertCoin: A NameCoin based decentralized authentication system.Technical Report, MIT, Class 6,857 Project,2014.
4. Fromknecht C, Velicanu D. A decentralized public key infrastructure with identity retention. MIT, Class 6,857 Project, 2014.
5. Lewison K, Corella F. Backing rich credentials with a blockchain PKI. Technical Report, Pomian & Corella, LLC, 2016.
6. E. Heilman, A. Kendler, A. Zohar, S. Goldberg. "Eclipse attacks on Bitcoin's peer-to-peer network." Usenix Conference on Security Symposium USENIX Association, 2015, 129-144.
7. I. Eyal,E.G. Sirer. “Majority is not enough: Bitcoin mining is vulner-able.” in Proc.Int.Conf.Financial Cryptography and Data Security.2014, 436-454.
8. A.Sapirshtein,Y.Sompolinsky, A.Zohar.Optimal selfish mining strategies in bitcoin,in Proc.Int.Conf.Financial Cryptography & Data Security,2016, 515-532.
9. Rosenfeld M. Analysis of Bitcoin Pooled Mining Reward Systems[J]. Computer Science, 2011, arXiv, 1112.4980.
10. Courtois N T, Bahack L. On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency [J]. Eprint Arxiv, 2014.
11. Chepurnoy A. Interactive Proof-of-stake[J],2016, arXiv,1601.00275.
12. Hurlburt G. Might the Blockchain Outlive Bitcoin[J]. It Professional, 2016, 18(2),12-16.
13. Garcia-Alfaro J, Herrera-Joancomart íJ, Lupu E, et al. Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance[J]. Lecture Notes in Computer Science, 2016, 8872.
14. M. Spagnuolo, F. Maggi, and S. Zanero. BitIodine: Extracting Intelligence from the Bitcoin Network, in Proc. Financial Cryptography, LNCS, 2014,vol(8437),457-468.
15. J. H. Joancomart, Research and Challenges on Bitcoin Anonymity,in Proc. the 9th Int. Workshop on Data Privacy Management,2014,3-16.
16. Moser M, Bohme R, Breuker D. An inquiry into money laundering tools in the Bitcoin ecosystem[C],Ecrime Researchers Summit. IEEE, 2014,1-14.
17. S. Feld, M. Schönfeld, and M. Werner.Analyzing the Deployment of Bitcoin’s P2P Network under an AS-level Perspective,in ANT/SEIT,ser.Procedia Computer Science,2014,vol(32),1121-1126.
18. P. Koshy, D. Koshy, and P. McDaniel. An Analysis of Anonymity Bitcoin Using P2P Network Traffic, in Proc. Financial Cryptography, 2014,vol(8437),469–485.
19. Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of Bitcoins: characterizing payments among men with no names[J]. Communications of the ACM, 2016,59(4),86-93.
20. Huang B, Liu Z, Chen J, et al. Behavior pattern clustering in blockchain networks[J]. Multimedia Tools & Applications, 2017, 76(19),1-12.
21. Zhu lihuang, Gao feng, et al. Overview of research on block chain privacy protection [J]. Computer research and development, 2017, 54(10), 2170-2186.
22. Li kang, Sun yi, Zhang jun, Li jun, Zhou jihua, Li zhongcheng. Technical challenges in the application of zero knowledge proof to block chain [J]. Big data, 2014,4(01),57-65.
23. Halpin H, Piekarska M. Introduction to Security and Privacy on the Blockchain[C], IEEE European Symposium on Security and Privacy Workshops. IEEE, 2017,1-3.

24. Herlihy M. Atomic Cross-Chain Swaps[J]. PODC '18 Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing, 2018, 245-254.
25. Wang H, Cen Y, Li X. Blockchain Router: A Cross-Chain Communication Protocol[C], IEEA '17 Proceedings of the 6th International Conference on Informatics, Environment, Energy and Applications, ACM, 2017, 94-97.