A Cross-Chain Identify Authentication Scheme Based on Block Chain

Yue Yu and Shibin Zhang(✉)

School of Cyberspace Security, Chengdu University of Information Technology, Chengdu, Sichuan, China
cuitzsb@cuit.edu.cn

Abstract. With continuous development of block chain technology, produced to visit each other between different blocks, chain requirements, cross chain has been becoming the current hot, there are four mainstream across chain technology, but have some problems, such as notary mechanism problems such as centralized, hash locking has such problems as low efficiency, aiming at the existing problem of the two, This paper proposes a combination of notary mechanism and hash-locked block chain cross-chain identity authentication scheme, a three-step cross-chain identity authentication model, strengthen the management of notary, strictly control the election of notary, and its security analysis, and finally carries out a further prospect to the scheme.

Keywords: Block chain · cross-chain · hash-lock · notary system

1 Introduction

With the continuous development of the block chain network, the demand for integration between various block chain projects is increasing, and the demand for cross-chain interaction is becoming more and more strong. How to break through the bottleneck of underlying performance and function and realize cross-chain interaction between different block chain has become the focus and difficulty of current research [5].

In the early stage of the development of block chain, research was conducted based on the form of single chain. However, due to the poor performance and scalability of single chain, it gradually transitioned to the research stage of multi-chain collaborative development [10]. Thus, four mainstream cross-chain technologies were derived, namely notary mechanism, hash locking, side chain/relay, and distributed key control. Currently, the notary mechanism is represented by Ripple's Interledger project [1], which allows for the transfer of assets and exchange of value between two different block chains through third-party connectors. Wang et al. [7] put forward the concept of block chain router, which can dynamically analyze and transmit communication requests according to communication protocols, maintain block chain network topology and realize inter-chain communication. Hash locking is a cross-chain technology to realize the exchange of assets between different chains. It requires the middleman and receiver of the transaction to give the correct hash value within a given time, representing the project as lightning network.

Z. Zeng et al. (Eds.): ECIT 2022, AHE 11, pp. 635–643, 2023.
https://doi.org/10.2991/978-94-6463-005-3_65

Table 1 Variable description.

Variable symbol	Variable meaning
ID$_a$	Alice’s account address
ID$_b$	Bob’s account address
Sig$_a$	Alice’s signature
Sig$_b$	Bob’s signature
TC	Content of this transaction
RT$_b$	Bob’s reasons for not participating in the transaction The amount of currency that Alice trades
1BTC	Alice’s payment to a notary
Re$_a$	Random numbers generated by Alice
s	The hash of a random numbers
h	Bob sets a new lock time, and t’ $<$ t
t’	The amount of currency that Bob trades
10ETH ToE	Bob’s offer for the deal

According to demand across the chain, this paper according to the center of the notary mechanism is not reliable, the problem such as security, atomicity, and hash locking problem such as the low efficiency of identity authentication model in this paper, a three phase across the chain, the notary system and hash locking effective integration, further enhance the efficiency of the trading across the chain, guarantee the safety of authentication across the chain. Variables used in this paper are shown in Table 1.

2 Related Technologies

2.1 Introduction to Block Chain Technology

Block chain technology was first born in the article Bitcoin: A Peer-to-peer Electronic Cash System published by Satoshi Nakamoto in 2008 [4]. It is an Internet technology abstracted from the digital currency Bitcoin. But block chain is not the same as bitcoin, which is just a cryptocurrency based on block chain technology.

Some people say that block chain technology is the next generation of value Internet, while others say that block chain technology is the world’s slowest database. Historically, few technologies have been as controversial as block chain technology. Different from traditional Internet technology, block chain technology is essentially a distributed ledger, which is a special data structure linked by one block. The biggest feature of block chain technology is decentralization. Every node in the system participates in the maintenance of the system, without the participation of a third party, which greatly reduces the security problems caused by the centralization of traditional Internet technology. Cryptography technology, as a technical support block chain, to block chain technology has the characteristic of tamper-resistant, traceability, by hash algorithm makes once all data on the chain can't change it, at the same time using hash the unidirectional and irreversible PengZhuangXing resistance makes the data, which makes the block chain technology is very safe and reliable, the current block chain technology are widely used in various fields.

2.2 Introduction to Block Chain Cross-Chain Technology

The so-called cross-chain is to make the value cross the barriers between chains through some technologies, so that the value originally stored in a specific block chain can be converted into the value on another chain, so as to realize the circulation of value. At present, the existing block chain projects in the market are all heterogeneous block chain developed by different teams according to different scene requirements and design concepts, and using different technical architectures. Based on the technical characteristics of block chain itself, each block chain is an isolated P2P network, so these projects are like an isolated “information island”. How to realize the interconnection and value transfer between block chain has become the research focus of the current block chain technology. If consensus mechanism is the core of block chain, then cross-chain technology is the key to realize interconnection and value transfer between isolated block chains. At present, there are four mainstream cross-chain technologies, which are notary mechanism, side chain/relay chain, hash locking, and distributed private key control. This paper mainly studies the notary mechanism and hash locking, and proposes a cross-chain identity authentication technology of block chain.

2.2.1 Notary System

The notary mechanism, also known as the witness mechanism, is to elect one or a group of trusted nodes as notary to verify whether a specific event has occurred on the block chain Y and prove it to the nodes on the block chain X. The notary community can reach a consensus on whether the event happened or not through a specific consensus algorithm. Notary model is the most widely used model at present, the largest single notary is the exchange. Notary mechanism is one of the easier solutions to achieve interoperability between block chains. It is easy to connect with existing block chain systems without complicated proof of work or proof of interest.

2.2.2 Side Chain/Relay

Side chain is a concept relative to the main chain. The formal definition of “side chain” by Block stream is that “side chain is a block chain verifying data from other block chains” [6]. The side-chain protocol is essentially a special cross-chain solution. This solution enables value transfer from chain X to chain Y and later from chain Y back to chain X. Chain X is usually referred to as the main chain and chain Y as the side chain. When there is a bottleneck in the performance of the main chain or some functions cannot be extended, the assets are transferred to the side chain, and relevant transactions can be executed on the side chain, so as to share the pressure of the main chain and expand the performance and function of the main chain.

2.2.3 Hash Locking

Hash locking [3] first appeared in the solution of Bitcoin Lightning network. It mainly realizes cross-chain transactions by locking assets and setting a fixed time and unlocking conditions. Assuming that the cross-chain transaction of Alice's 1BTC and Bob's 10ETH is now completed, the basic process of hash locking is as follows:

(1) Alice, the account on chain X, first generates a random number S, and gives the hash(s) of the random number S to Bob, the account on chain Y;
(2) Account Alice locks asset 1BTC on chain X, and sets corresponding conditions. If chain X receives S within time TA (current time + 2X), the money will be transferred to account Bob, otherwise the asset will be returned to account Alice;
(3) After account Bob receives hash(s) and sees the locking time and corresponding conditions set by account Alice, asset 10ETH is locked on chain Y. A condition is also set that if chain Y receives a random number S in time TA-x, it will be transferred to account Alice; otherwise, it will be returned to account Bob;
(4) After account Alice sees the locking condition of account Bob, she sends S to chain Y in time TA-x to obtain the asset 10ETH of chain Y;
(5) After account Bob receives the random number S, he sends S to chain X within time TA to obtain the asset 1BTC of chain X. At this point, the transaction is completed.

2.2.4 Distributed Control Key

Distributed private key control the private keys of various assets are controlled by distributed nodes, and the original chain assets are mapped to the cross-chain to ensure that all kinds of assets can be interconnected in the blockchain system. The core of distributed private key control is distributed control management, that is, the ownership and use rights of assets are separated, and the control rights of digital assets on the original chain are safely transferred to the decentralized system [8]. Distributed private key control is similar to notary mechanism, but the user always has the control over the asset, but the distributed storage method is adopted to store the key of digital asset, which avoids the centralized risk under notary mechanism to a certain extent [9]. In addition, account locking does not require bidirectional anchoring. All transactions are introduced into the original chain network after the verification node reconstruction, without changing the characteristics of the original chain, and all chains can access the original chain freely and with low threshold, reducing the cost of cross-link entry. Therefore, it is widely applicable and easy to implement. However, since the characteristics of the original chain are not changed, cross-chain development needs to be adapted to the characteristics of the original chain, so the development is difficult and the confirmation of the original chain takes a long time, resulting in low operation efficiency [2].

3 A Cross-Chain Identity Authentication Model for Block Chain

3.1 Cross-Chain Identity Authentication Model

Aiming at the problems of the existing notary mechanism and hash locking, this paper proposes a cross chain identity authentication model of block chain, which is shown in Fig. 1.

3.2 Cross Chain Identity Authentication Process

The whole process is divided into three stages, namely, identity authentication stage S1, pre transaction stage S2 and formal transaction stage S3. The same assumption is that Alice and Bob from different block chains are authenticated by notaries and exchanged between 1btc and 10eth.

3.2.1 Identity Authentication

This stage is mainly to complete the identity authentication of both parties and to conduct the election of notaries.

(1) Alice, the user on the source chain, proposes an authentication application {Ida, Siga}, and sends the application to the system.
(2) After receiving the application, the nodes in the system will start to run for notaries.
(3) The elected notary checks the application sent by Alice, checks its identity information and saves it, and forwards the application to the target chain.
(4) Bob, the user in the target chain, receives the application, also submits the application for identity authentication {IDb, Sigb}, and sends the application to the notary office, and the notary also checks and saves its identity information.

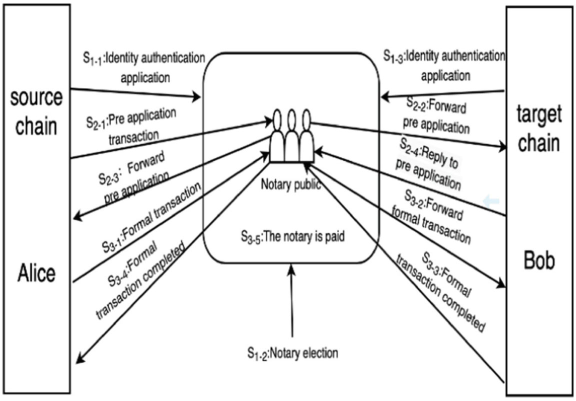
source chain
Alice
$S_{1\text{-}1}$:Identity authentication application
$S_{2\text{-}1}$:Pre application transaction
$S_{2\text{-}3}$: Forward pre application
$S_{3\text{-}1}$:Formal transaction
$S_{3\text{-}4}$:Formal transaction completed
Notary public
$S_{3\text{-}5}$:The notary is paid
$S_{1\text{-}2}$:Notary election
$S_{1\text{-}3}$:Identity authentication application
$S_{2\text{-}2}$:Forward pre application
$S_{2\text{-}4}$:Reply to pre application
$S_{3\text{-}2}$:Forward formal transaction
$S_{3\text{-}3}$:Formal transaction completed
target chain
Bob

Fig. 1. Cross chain authentication model

3.2.2 Pre Transaction

This stage mainly informs the node Bob on the target chain of the transactions to be initiated to decide whether to conduct the next stage of transactions.

(1) Alice put forward the pre transaction application {IDa, IDb, Siga, TC}, broadcast the application to the system and target chain, and the notaries elected to view the application contents and forward it to Bob, the target chain user.
(2) Bob can choose whether to conduct the transaction according to the transaction content after receiving the transaction request. If it decides to participate in the transaction, he/she will attach his signature Sigb to the notary in the transaction application. If he does not participate in the transaction, the reason for not participating in the transaction will be attached to the transaction application to the notary.
(3) After receiving the transaction list returned by Bob, the notary public will check whether Bob participates in the transaction according to the contents of the list, so as to determine the destination of the N notaries elected, and send the return list to Alice. After Alice receives the return list, it decides whether to conduct the next stage of transaction according to the contents of the list.

3.2.3 Formal Transaction

This stage is the most important stage of the whole process, which is formally related to asset transfer.

(1) Alice carries out the next transaction according to the received return list. At this time, Alice sends a formal transaction TX {IDa, IDb, Siga, TC, 1BTC, Rea, h}, but at this time, the reward Rea that Alice pays to the notary is locked by Alice. At the same time, Alice sets a locking time t, and then sends the transaction list to the notary.
(2) After receiving the formal transaction request, the notary looks at the transaction content, reconfirm the identity information of the transaction applicant and the authenticity of the transaction, then takes out the transaction amount 1btc and locks it, and immediately forwards the transaction to Bob (here, it is set that the time for the notary to forward to Bob is far less than the locking time t).
(3) After Bob receives the transaction, he sends {IDb, IDa, Sigb, 10ETH, ToE, Reb, t'} to the notary according to the content of TX. But at this time, the remuneration Bob pays to the notary is locked by Bob, and the notary takes out the transaction amount 10eth and forwards it to Alice.
(4) After receiving the transaction, Alice provides a random number s according to the transaction conditions proposed by Bob to get the hash value H, which is sent to the notary. After the notary's verification is successful, Alice can successfully take away 10eth and release the reward rea paid to the notary.
(5) At this time, the notary sends the random number s to Bob. At this time, Bob can take 1btc according to the random number, and release the reward Reb paid to the notary. At this point, the transaction ends.

3.3 Election and Management of Notaries

(1) In order to improve the security of cross chain identity authentication and prevent the abuse of the rights of a single notary, n notaries will be selected every time the notaries are elected. The rights of each notary elected are equal, and every node in the system can participate in the election of notaries;
(2) The first n notaries who are elected each time must have a credit value greater than the initial value n;
(3) The incentive mechanism is introduced to reward the nodes that make contributions in the cross chain process, and punish the nodes that do not work or do evil. When a node successfully completes the work of a notary, it will get a certain reward. The reward can be converted into the corresponding credit value according to the conversion rules. When the credit value of a node is less than 1/2n, The node no longer has the qualification of running for notaries for a certain time t;
(4) In order to prevent the top n notaries ranking the top, the other nodes can not be notaries, and the problem of notaries' group appears, the system will set all the credit values of all nodes as the initial value for a period of time, and make a new round of reputation ranking.

4 Safety Analysis

This paper proposes a cross chain identity authentication scheme based on block chain. According to the problems of traditional cross chain mechanism, reputation ranking and incentive mechanism are introduced, and hash locking is integrated into the model to further ensure the security in the process of cross chain transaction.

4.1 The Problem of Notary's Crime

By electing multiple notaries, the centralization of traditional notary mechanism is weakened, and the problem of single notary's crime in the process of authentication is avoided.

4.2 Reputation Value

By introducing reputation value ranking, the election of notaries can be changed to better ensure the enthusiasm of each node to participate in the election and the security of the system.

4.3 Incentive Mechanism

By introducing incentive mechanism, more nodes are encouraged to participate in the transactions in the system, so as to further ensure the security of the system.

5 Summary and Prospect

5.1 Summary

According to the existing problems of cross chain technology, this paper proposes a cross chain identity authentication method based on the combination of notary mechanism and hash locking, which integrates hash locking into the notary man-machine system, sets the locking time, improves the efficiency of authentication, and solves the problem of notary centralization by electing multiple notaries. At the same time, it further introduces the reputation ranking and incentive mechanism, the security of authentication is guaranteed.

5.2 Prospect

The three-stage cross chain identity authentication proposed in this paper is only a preliminary scheme design, and there are still some problems, such as the group crime of notaries, hash lock timeout and so on, which will be further analyzed and studied in the future research.

References

1. Ang W (2019) An improved blockchain cross-chain technology. Cyberspace Secur 10(06):40–45
2. Fusion (22 May 2022) Fusion: An inclusive cryptofinance platform based on blockchains [EB/OL]
3. Herlihy M (2018) Atomic cross-chain swaps. In Proceedings of the 2018 ACM symposium on principles of distributed computing, pp 245–254
4. Nakamoto S (2008) A peer-to-peer electronic cash system. Bitcoin. https://bitcoin.org/bitcoin.pdf
5. Shuai H, Xiangnian H, Xiaoliang C (2021) Review on the development and application of blockchain cross-chain technology. J Xihua Univ (Nat Sci Edn)
6. Buterin V. (n.d.) Chain Interoperability [EB/OL]. https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdfi. Accessed 9 Sept 2016/7 Apr 2019
7. Wang H, Cen Y, Li X (2017) Blockchain router: a cross-chain communication protocol. In Proceedings of the 6th international conference on informatics, environment, energy and applications
8. Yie A, Casallas R, Deridder D et al (2012) Realizing model transformation chain interoperability. Softw Syst Model 11(1):55–75
9. Guo Z, Guo S, Zhang S, Song L, Wang H (2020) J. Internet Things 4(02):35–48
10. Zhuoyan X, Xuan Z (2020) Overview of cross-chain technology development. Comput Appl Res 38(2):341–346