Cross-Chain Model of Notary Group Based on Verifiable Random Functions

Can OuYang[1(✉)] and Xiaohong Qiu[2]

[1] Jiangxi University of Science and Technology, Nangchang 330013, China
ouyangcan0127@163.com
[2] Nanchang Key Laboratory of Virtual Digital Factory and Cultural Communications, Nanchang 330013, People's Republic of China

Abstract. In response to the issues of high centralization, slow transaction rates, and high security risks in the cross-chain mechanism of notary groups, this paper proposes an identity-based, non-interactive cross-chain model for notary groups. The model introduces notary groups to reduce centralization and divides the nodes within the notary group into transaction nodes, validation nodes, and supervisory nodes using verifiable random functions, significantly improving the fault tolerance of the optimized model. Additionally, the model introduces Merkle tree structures to locally store transaction information, enabling the processing of multiple cross-chain transactions at once and reducing transaction latency caused by multiple verifications, thereby improving transaction rates. Experimental results demonstrate that compared to traditional models, the optimized model significantly reduces transaction security risks and increases transaction rates by 55.8%.

Keywords: blockchain · blockchain · verifiable random function · notary mechanism

1 Introduction

With Bitcoin becoming a hot topic of discussion, Blockchain 1.0 quietly arrived, and society entered the era of blockchain. The emergence of open-source platforms like Ethereum [1] enabled various industries to combine the characteristics of blockchain technology, such as decentralization, high security, and immutability, with their specific industry requirements. The continuous implementation of various DApps also heralded the arrival of the blockchain 2.0 era. As blockchain 3.0, represented by EOS, became the core of value interconnection, every piece of information and byte representing value in the Internet can undergo ownership confirmation, measurement, and storage, enabling assets to be tracked, controlled, and traded on the blockchain. However, in different application scenarios, issues such as information circulation and large-scale blockchain data storage have emerged, often requiring costly third-party fees to address. With the advent of cross-chain technology, the consumption of financial and material resources has been reduced, facilitating asset interaction and information circulation.

C. Wu et al. (Eds.): MONAMI 2023, LNICST 559, pp. 45–54, 2024.
https://doi.org/10.1007/978-3-031-55471-1_4

Currently, numerous implementation solutions have been proposed for cross-chain technology. The founder of Ethereum has put forward three different implementation methods for cross-chain technology [2]: the notary mechanism, sidechain/relay chain technology, and hash locking technology. Additionally, as the number of blockchain applications increases, a new cross-chain technology called distributed private key control has emerged. The notary mechanism is relatively simple to implement but overly relies on the trust of notaries, leading to low security and high centralization. Sidechain/relay chain technology primarily extends the main chain and its security depends on the main chain, but it imposes certain requirements on the structures of the cross-chain parties, making it challenging to implement. Hash locking technology is widely used and achieves cross-chain asset exchange through smart contracts, but it is limited in its ability to transfer assets. Distributed private key control technology separates asset ownership and usage rights to facilitate asset circulation and value transfer between heterogeneous chains, offering high security but posing challenges for implementation and wider adoption.

Compared to the other three cross-chain technologies, the notary mechanism has lower costs, is easy to implement, and is suitable for large-scale application in various scenarios. Therefore, this paper proposes an improved cross-chain model using a notary group to address the issues of high centralization, slow transaction rates, and high security risks in traditional notary cross-chain mechanisms.

2 Blockchain Cross-Chain Technology

In blockchain, each node typically joins an independent blockchain network, and different blockchain networks, in their initial design and development, do not support interconnectivity and lack the characteristic of the Internet of Everything. To promote interconnection in blockchain and prevent different blockchain networks from being value silos, cross-chain technology has gained increasing attention. The following will introduce four common types of cross-chain technology.

2.1 Notary Scheme

The Notary Mechanism refers to the introduction of a trusted third-party notary node between mutually untrusted blockchains. This notary node is responsible for verifying the consistency and legality of the transaction information exchanged between the parties.

The specific process is as follows: Firstly, a user, Alice, on Chain A transfers the assets to the notary node. The notary node verifies and locks Alice's assets. Finally, the transaction information is confirmed by Bob on Chain B to complete the transfer of the previously confirmed and locked assets. The Notary Mechanism operates on a simple principle without the need for complex Proof-of-Work (PoW). However, the simplicity of the Notary Mechanism's structure and its high reliance on notary nodes result in a higher degree of centralization. Many scholars also question its compatibility with the decentralized nature of blockchain. Currently, the representative projects of mature Notary Mechanisms include Interledger [3, 4].

2.2 Sidechain/Relay Chain Technology

Currently, there are mature cross-chain projects implemented using Sidechain/Relay Chain Technology. These include Rootstock and BTC-Relay [5], both of which are considered sidechain solutions that enhance the performance of the Bitcoin network. In this approach, the existing running blockchain network serves as the main chain, while the sidechain is constructed on top of it by anchoring to the main chain. The main chain offloads its pressure to the sidechain, thereby improving its own performance and scalability. To alleviate the pressure on the Bitcoin mainnet and increase virtual currency payment channels, the BTC-Relay project was proposed as a solution using Sidechain/Relay Chain Technology. It enables one-way cross-chain payments using Bitcoin on the Ethereum network, reducing the limitations of transactions and effectively addressing issues such as low throughput and long transaction confirmation times in the Bitcoin network.

In the Relay Chain cross-chain model, the relay chain acts as a forwarding hub that simply relays transactions without the need to maintain data. It can be regarded as a network hub. Moreover, in the forwarding of inter-chain transaction information, the receiving party verifies the messages without the need to download block header data, which improves the transmission speed. The flexibility and scalability of the relay mode are unique compared to other cross-chain solutions. One of the currently mature relay cross-chain solutions is Cosmos [6].

2.3 Hash Locking Technology

Time locks and hash locks are the core components of Hash Locking Technology [7]. When using hash locks to lock user assets on the corresponding chain, a time lock is also set to restrict the transaction within a specified time period. The time lock ensures that only if both parties provide the correct hash value within the designated transaction time, the assets can be unlocked and the transfer can be completed. The Lightning Network [8] utilizes hash locking technology to address issues such as low transaction throughput and long confirmation times in the Bitcoin network, optimizing Bitcoin transactions through off-chain channels.

While Hash Locking Technology achieves asset exchange between heterogeneous chains by reducing the amount of information disclosed between transaction parties and minimizing their knowledge of each other, there are still challenges that need to be addressed, including low transaction efficiency, high payment costs, and limited scalability.

2.4 Distributed Private Key Control Technology

The core idea of Distributed Private Key Control Technology is to map the assets of different nodes onto an intermediate chain and achieve interoperability between various blockchain networks through the distributed control of private keys by multiple nodes. This technology enables the seamless exchange of assets between different blockchains by allowing distributed nodes to control the private keys associated with each node.

Distributed Private Key Control Technology shares many similarities with the notary mechanism in terms of the overall process. However, in the context of distributed private key cross-chain solutions, users retain control over their own assets. Similar to the notary mechanism, this technology offers broad applicability and ease of implementation.

Representative projects implementing this technology include Wanchain and Fusion [9].

2.5 The Current State of Improvements in the Notary Mechanism

Currently, scholars such as Xue [10] have proposed improvements to the traditional notary model to address issues such as high centralization, slow transaction speed, and high security risks. They have introduced a cross-chain interaction model based on a notary group. Compared to the traditional notary cross-chain model, the complexity of the transaction result's signature count has been reduced from O(n) to O(1), thus lowering the degree of centralization in the notary mechanism. Additionally, this model does not require the verification of every transaction, leading to improved transaction speed.

Scholars like Dai [11] have collected relevant information about multiple notary nodes and utilized an improved PageRank algorithm to rank the credibility of these nodes. By prioritizing highly credible notary nodes for transactions, the security of the model is enhanced.

Cao [12] proposed a cross-chain data traceability mechanism for addressing the issue of data flow across different trust domains. The mechanism establishes a cross-domain access and traceability mechanism by constructing a global authorization chain and access chains within each trust domain. By integrating cross-chain technology based on notary groups, the mechanism enables global authorization and transactions of data assets, as well as cross-domain data access and traceability.

3 VRF-Based Notary Group Cross-Chain Model

In response to the high degree of centralization, slow transaction speeds, and high security risks in the public notary group cross-chain mechanism, this paper proposes an improved model of the public notary group cross-chain mechanism based on Verifiable Random Function (VRF). The model consists of four parts: the public notary group, VRF-based random selection, public notary incentive mechanism, and Merkle tree verification.

Unlike the traditional public notary group model where all notary nodes have the same functions, the optimized model divides the notary group nodes into three categories: validation nodes, transaction nodes, and supervisory nodes. In the mechanism for extracting node identities, the current interactive validation scheme for node identity disclosure is vulnerable to attacks and lacks security. The optimized model introduces VRF-based random selection function to locally extract node identities. Transaction nodes only need to provide a proof pi, generated from the private key SK and a random number alpha, to all supervisory nodes for identity verification. This prevents precise attacks on nodes and improves security. Unlike traditional public notary cross-chain interaction models, the optimized model proposed in this paper ensures that even if a

single node is attacked or goes offline, as long as the number of malicious nodes does not exceed half of the transaction nodes, it does not impact the transaction results. It possesses a Byzantine fault tolerance of $f = 2n + 1$.

3.1 Cross-Chain Model of the Public Notary Group

For the issues encountered in the traditional notary model, we have implemented the following optimizations:

1) Introducing a public notary group and dividing the notary nodes' roles to reduce the centralization and single point of failure issues in the traditional notary model.
2) Utilizing the VRF algorithm to partition the nodes' identities, with the remaining nodes acting as verification nodes and supervision nodes for validating the legitimacy of transactions and the identities of transaction nodes. This prevents identity spoofing attacks and enhances the security of the model.
3) Instead of querying the blockchain for each transaction during information verification, we construct a Merkle tree locally to enable fast verification of block data. This reduces communication and computational overhead, thereby improving transaction speed.

The specific cross-chain process is illustrated in Fig. 1.

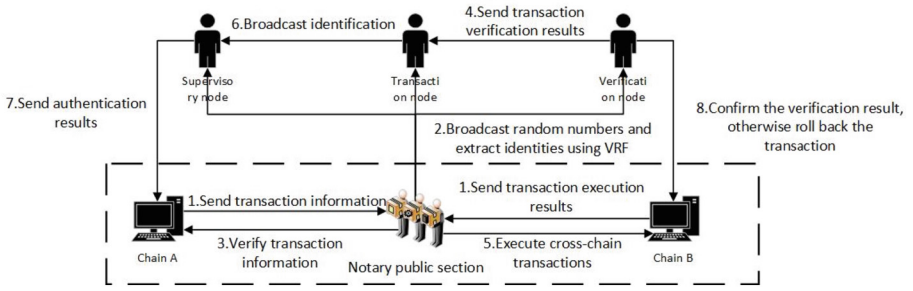

Fig. 1. Cross-chain Transaction Process Flowchart

In Fig. 1, the traditional model is described in detail using dashed boxes, while the optimized model makes certain improvements in certain steps compared to the traditional model. The specific descriptions are as follows:

1) When the cross-chain group receives the transaction information, it proceeds to Step 2. All nodes in the group perform a hash operation on the random number alpha broadcasted by the system and extract their node identities using the VRF algorithm. Unlike the traditional model where node identities are publicly known, in each cross-chain operation, no one can determine the exact identity of the transaction node. Each node only knows its own identity and verifies the broadcasted identity proof pi. This effectively solves the problem of malicious attacks resulting from the public disclosure of node identities in the traditional model.

2) After the completion of Step 2, the verification nodes perform a breadth-first search on the local Merkle tree structure to quickly verify the legality of the transaction. After each merge of the local Merkle tree to obtain the Merkle tree root node, it is compared with the Hash value and PreHash value in the block header of Chain A. Compared to the traditional model that directly compares and searches for the Hash value in the block header of Chain A, the optimized model reduces a significant amount of ineffective searches and reduces system redundancy.
3) Regarding transaction confirmation, the optimized model adopts a dual verification mechanism. In addition to verifying the legality of the transaction information in the traditional model, the optimized model includes the verification of the transaction node identity, as shown in Steps 7 and 9 in Fig. 1. A cross-chain request can only succeed if both types of verification yield positive results. Otherwise, the transaction will be rolled back through the execution of smart contracts using the SDK provided by both transaction chains, thereby enhancing system stability.

3.2 Verifiable Random Functions

The verifiable random function (VRF), proposed by Silvio et al. [20], is an encryption scheme that maps inputs to verifiably pseudo-random outputs. For a given input random value *alpha*, different nodes output a corresponding random value *beta* and a random proof *pi* based on their own private key *SK*, the specific functions are as follows:

$$beta = VRF\_Hash(SK, alpha) \tag{1}$$

$$pi = VRF\_Prove(SK, alpha) \tag{2}$$

As for the random value *beta*, it can be verified using the proof *pi* as input through the *Proof*2*Hash* function.

$$beta = Proof\,2Hash(pi) \tag{3}$$

For the generated random value of *beta*, the range of values is: $beta \in [0, 2^{bits(beta)}]$, Since VRF cannot accomplish a fixed number of drawing tasks, the algorithm introduces a new threshold *gamma*. By adjusting the value of *gamma*, the probability of selecting transaction nodes can be modified. When the *beta* is divided by $2^{bits(beta)}$ is less than *gamma*, the node is selected as a transaction node. VRF requires different private keys from different transaction nodes, which ensures that each node generates unique *beta* and *pi* values. This prevents the design of a unified standard that would make a random result uniquely meet a certain condition. It also enhances resilience against external attacks on transaction nodes.

$$result = VRF\_Verify(alpha, beta, pi, PK) \tag{4}$$

The validation result of the transaction node's identity is obtained through *VRF_Verify*, and *pi* provides a zero-knowledge proof for the validation of the random value, which includes the private key signature of the generator. The verifier calculates the hash by using the globally broadcasted random number alpha and the public key *PK* of the transaction node, then compares the result with the output random number to obtain a Boolean value, *result*, for the validation of the transaction node's identity.

4 Analysis of Experimental Results

4.1 Software and Hardware Test Environment

The software and hardware environment for the testing in this paper is shown in Table 1.

Table 1. The software and hardware testing environment.

Name	Version/Model
OS	macOS Monterey (12.3)
CPU	2 GHz 4 Core Inter Core i5
RAM	16 GB 3733 MHz LPDDR4X
Programming language	Golang 1.17.8
Blockchain framework	Fabric 2.4.3, FISCO BCOS 2.7.1

4.2 Experiment and Result Analysis

Identity Extraction Experiment

After a detailed analysis of VRF in Sect. 3.2, it is not difficult to determine that the selection of transaction nodes is completely random. There is also a certain probability of having zero transaction nodes, which is calculated as $p = (1 - gamma)^{n}$. The model can adjust the probability of notary nodes being selected as transaction nodes by setting an appropriate threshold value, *gamma*. Due to hardware limitations in the experimental environment, the maximum number of deployable notary nodes in the current setup is 13, with a CPU usage rate reaching 95.6%. Under the condition of ensuring the normal completion of the experiment without any crashes, the impact of different numbers of notary nodes and the values of *gamma* on the absence of transaction nodes was analyzed. The analysis results are shown in Fig. 2.

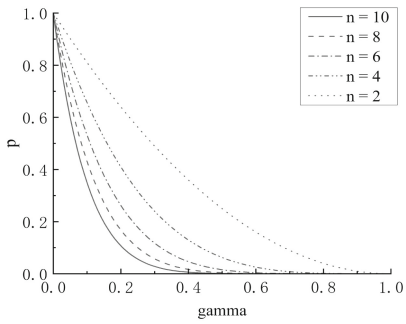

Fig. 2. No transaction node probability graph is generated

The analysis of Fig. 2 reveals that when *gamma* is fixed, the probability of no transaction nodes decreases as the value of n increases. When the value of n is fixed, the probability of no transaction nodes decreases as the value of *gamma* increases. Under the condition of fully utilizing resources, this paper sets the number of notary nodes to n = 10. Analyzing the curve for n = 10 in Fig. 2, it is observed that as *gamma* increases, the downward trend of p becomes stable when *gamma* reaches around 0.4. Therefore, in the subsequent experiments, $gamma = 0.4$ is set as a constant, under which the theoretical probability of not generating transaction nodes is 0.0001. To address the situation of no transaction nodes being generated, the optimized model sets up a transaction timer within the notary node group. When a transaction request is received, the timer starts counting, and if no transaction nodes are generated within the set time, a new round of identity extraction is initiated. In this case, the probability of no transaction nodes occurring is given by $p = (1 - gamma)^{2n}$. The specific test results are presented in Table 2.

Table 2. No transaction node statistics table

Number Of Transaction	Set Transaction Timer(Y/N)	Transaction Node Not Specified
1000	N	1
10000	N	8
1000	Y	0
10000	Y	0

Based on the experimental data statistics, it is observed that when the transaction timer is not set within the notary group, the probability of having no transaction node is 0.08%. However, after implementing the transaction timer within the notary group, the occurrence of no transaction node is eliminated.

Defense Against Malicious Attack Experiment

To test the system's ability to resist malicious node improvements, we set the number of nodes in the notary group as n = 10, with half of the nodes being malicious and the other half being normal. We conducted separate tests to evaluate the transaction security of both the traditional notary group cross-chain model and the optimized model under malicious conditions. The experimental results are shown in Fig. 3.

The experimental results indicate that when the number of malicious nodes reaches 50% of the total number of nodes in the notary group, all initiated transactions fail with a probability of 100%. The optimized model outperforms the traditional model when facing attacks. Analyzing the experimental results reveals that the average number of transaction failures in the VRF-based notary group model decreases by 94% compared to the traditional model. With an increase in the number of transactions, the failure rate slightly increases, averaging at 6%. This demonstrates a significant improvement in the ability to resist malicious attacks.

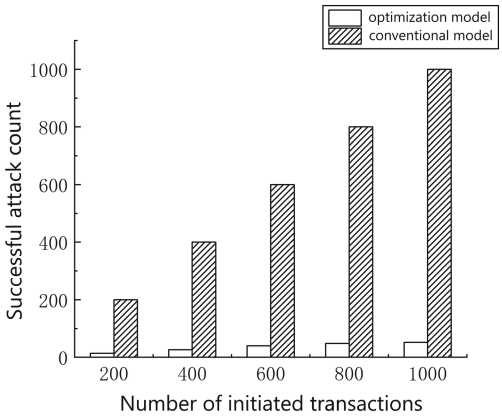

Fig. 3. Number of successful attacks by malicious nodes

5 Conclusion

This paper proposes a notary group cross-chain transaction model based on a random verifiable function to address the issues of low transaction efficiency, poor resistance to malicious attacks, and long verification time in traditional notary cross-chain mechanisms. The model is tested for the possibility of not generating transaction nodes and proposes the addition of a transaction timer to solve the problem of zero transaction nodes. Subsequently, the security and transaction processing time of the traditional model and the optimized model are tested, and the experimental results are analyzed and explained. The experimental results demonstrate that the improved notary mechanism, under the same hardware conditions, exhibits better security performance and faster transaction processing speed compared to the traditional notary mechanism.

References

1. Butterin, V.: Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform 2014 (2022)
2. Buterin, V.: Chain interoperability. R3 Research Paper, 9 (2016)
3. Schwartz, E.: A payment protocol of the web, for the web: or, finally enabling web micropayments with the interledger protocol. In: Proceedings of the 25th International Conference Companion on World Wide Web, pp. 279–280 (2016)
4. Hope-Bailie, A., Thomas, S.: Interledger: creating a standard for payments. In: Proceedings of the 25th International Conference Companion on World Wide Web, pp. 281–282 (2016)
5. Qun, W.A.N.G., Fujuan, L.I., Xueli, N.I., Lingling, X.I.A., Guangjun, L.I.A.N.G., Zhuo, M.A.: Research on blockchain interoperability and cross-chain technology. J. Front. Comput. Sci. Technol. **1**
6. Kwon, J., Buchman, E.: Cosmos: a network of distributed ledgers (2016). https://cosmos.network/whitepaper
7. Zhang, S.T., Qin, B., Zheng, H.B.: Research on multi-party cross chain protocol based on hash locking. Cyberspace Secur. **9**(11), 57–62
8. Poon, J., Dryja, T.: The bitcoin lightning network: scalable off-chain instant payments (2016)

9. Fujimoto, S., Higashikado, Y., Takeuchi, T.: ConnectionChain: the secure interworking of blockchains. In: 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 514–518. IEEE (2019)
10. Jiang, C., Fang, L., Zhang, N., Zhu, J.: Cross-chain interaction safety model based on notary groups. J. Comput. Appl. **42**(11), 3438–3443 (2022)
11. Dai, B., Jiang, S., Li, D., et al.: Evaluation model of cross-chain notary mechanism based on improved PageRank algorithm. Comput. Eng. **47**(2), 26–31 (2021)
12. Cao, L., Zhao, S., Gao, Z., Du, X.: Cross-chain data traceability mechanism for cross-domain access. J. Supercomput. **79**(5), 4944–4961 (2023)
13. Esgin, M.F., Steinfeld, R., Liu, D., Ruj, S.: Efficient hybrid exact/relaxed lattice proofs and applications to rounding and VRFs. In: Handschuh, H., Lysyanskaya, A. (eds.) CRYPTO 2023. LNCS, vol. 14085, pp. 484–517. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-38554-4_16
14. Xiong, A., Liu, G., Zhu, Q., Jing, A., Loke, S.W.: A notary group-based cross-chain mechanism. Digit. Commun. Netw. **8**(6), 1059–1067 (2022)
15. Sun, Y., Yi, L., Duan, L., Wang, W.: A decentralized cross-chain service protocol based on notary schemes and hash-locking. In: 2022 IEEE International Conference on Services Computing (SCC), pp. 152–157. IEEE (2022)
16. Wang, Z., Li, J., Chen, X.B., Li, C.: A secure cross-chain transaction model based on quantum multi-signature. Quantum Inf. Process. **21**(8), 279 (2022)
17. Chen, L., Fu, Q., Mu, Y., Zeng, L., Rezaeibagha, F., Hwang, M.S.: Blockchain-based random auditor committee for integrity verification. Futur. Gener. Comput. Syst. **131**, 183–193 (2022)