Dynamic Notary Group Election Algorithm Based on Reputation Value

Shoucai Zhao and Lifeng Cao(✉)

He'nan Province Key Laboratory of Information Security, Zhengzhou, China
shoucaizhao123@163.com, caolf302@sina.com

Abstract. As a distributed ledger technology, blockchain can be used in the fields of information sharing, logistics chain, certificate storage and anti-counterfeiting. However, due to the isolated nature of the blockchain network and the high degree of heterogeneity between chains, the connection between different chains is hindered, which makes each blockchain form a value island and cannot serve the practical applications well. The emergence of cross chain technology realizes the value circulation between different chains and enhances the interoperability and scalability of blockchains. Among them, the cross-chain technology of notary mechanism transforms the trust problem among cross-chain users into the loyalty problem of notary, and is favored for its ability to support different types of underlying blockchain systems in a more flexible manner. However, the introduction of notaries in the notary mechanism also leads to the risk of centralization, and the loyalty of notaries will directly determine the success of cross-chain transactions. In this paper, by introducing the improved PageRank algorithm, we design a dynamic notary group election mechanism based on reputation value, which effectively avoids malicious nodes from becoming notaries and improves the success rate of cross-chain transactions while preventing the over-concentration of rights in a single node. The experimental analysis shows that selecting notary representatives by dynamically adjusting the reputation value ranking of notary nodes increases the selection probability of loyal nodes, which is more reasonable than the method of randomly selecting notaries.

Keywords: Blockchain · Cross Chain · Notary Group · PageRank

1 Introduction

Blockchain is a decentralized, trustless distributed data ledger [8]. It allows all nodes in the network to jointly own, manage and supervise data through cryptographic methods, and the system operates without the control of any single node, thus having the characteristics of being unforgeable, untamperable and traceable. With the research and innovation of blockchain technology, more and more blockchain technologies are applied in the fields of information sharing, copyright protection, data traceability, financial asset transaction settlement, deposit certificate anti-counterfeiting and so on. Projects in different fields usually adopt different technical frameworks to develop blockchains with different architectures, Even different teams in the same field have developed many

D. Qiu et al. (Eds.): ICBBEM 2022, AHIS 5, pp. 903–915, 2023.
https://doi.org/10.2991/978-94-6463-030-5_89

blockchains with different architectures. The different chains in the blockchain are highly heterogeneous, each independent blockchain is a relatively independent network, data information can not be interconnected, and there is the problem of information silos [3]. In addition, the difficulty of collaboration among blockchain networks greatly limits the development of blockchain applications, so the interconnection and value transfer between blockchains has become an urgent problem, and thus cross-chain technology is born [10].

Blockchain cross-chain technology is an effective way to realize inter-blockchain interaction, which not only enables information flow between different blockchains, but also value transfer between different blockchains, which largely enhances the scalability of blockchain. Although there are various cross-chain technologies and cross-chain concepts being proposed, there are also certain problems. For example, in the traditional notary mechanism, the mechanism requires both parties to choose a node or a group of nodes that both parties trust as the "middleman", and both parties rely entirely on the "middleman" for cross-chain transactions. Although this cross-chain mechanism is the first proposed cross-blockchain approach and is more mature than other cross-chain technologies, it still has room for improvement.

Since the traditional notary mechanism depends entirely on the notary, the reliability of the notary determines the success of cross-chain transactions. The single-notary mechanism increases the risk of centralization, which is in contrast to the blockchain decentralization idea. In the existing multi-notary mechanism, the notaries are usually selected randomly, and if there are more malicious nodes in the randomly selected group of notaries, it is more likely to lead to transaction failure. Based on this, this paper introduces the concept of trust score, and different nodes vote for trust according to the high trust score. Then the average value of the trust score of each node is used as the initial reputation value, and the final reputation value of each node is calculated by combining the improved PageRank algorithm to finally determine the required group of notaries for cross-chain transactions. The improved PageRank algorithm constructs a dynamic notary group election model based on reputation value, realizes dynamic joining and quitting of nodes in the notary group, improves the probability of reliable nodes becoming notaries, and solves the trust problem of cross-chain user transactions while reducing the risk of centralization of the notary mechanism.

2 Mainstream Cross Chain Technology

Cross chain operation can be divided into cross chain between isomorphic chains and cross chain between heterogeneous chains. For the isomorphic chain, the consensus algorithm, block generation and verification rules, transaction broadcast, security mechanism and other logic of both parties are consistent, so the cross chain interaction is relatively simple. There are different consensus mechanisms and accounting methods between different chains. Reaching a security consensus is a technical difficulty and a challenge for many developers. The current cross chain schemes mainly include: Notary schemes, sidechains/relays, hash locking, distributed private key control and notary+side chain technology.

2.1 Notary Mechanism

The cross chain mechanism that introduces one or more trusted entities for credit endorsement is called notary mechanism. Notary mechanism is the simplest cross chain mechanism that can be realized technically [4]. When there is value circulation demand between different blockchains, select one or more nodes as notaries. The selected notaries are used to listen to the transaction requests on different chains, and finally respond by reaching a consensus on the occurrence or non-occurrence of the event through the existing consensus algorithm. According to the number of selected notaries, the notary mechanism can be divided into single signature notary and multi signature notary. According to the differences of signature methods, multi signature notary can be divided into multi signature notary mechanism and distributed signature notary mechanism.

2.1.1 Single Signature Notary

As the name suggests, the single signature notary mechanism has only one node as a notary. When there is a transaction demand between different chains, the notary shall collect, verify and confirm the transaction between different chains. Strong compatibility and fast processing speed are the unique characteristics of single signature notaries. However, since only one node acts as a notary, the node must be a trusted node to correctly complete cross chain transactions, which is contrary to the viewpoint of blockchain decentralization. Therefore, the notary group model is more used in practical applications to reduce the dependence on a single node.

2.1.2 Multi Signature Notary

The multi notary signature mechanism [6] is signed by multiple notaries on their respective account books, and the cross chain transaction can be completed only after reaching a consensus. When there is cross chain transaction demand between different chains, select some nodes from the notary group as notaries, and each notary selected has its own unique private key for signature. Only after a certain proportion of notaries sign, the transaction can be confirmed. Since multiple notaries participate in the transaction confirmation, the attack or evil of a few notaries will not affect the normal operation of the system, reduce the centralization risk and improve the anti attack ability of the cross chain system.

2.1.3 Distributed Signature Notary

The biggest difference between distributed signature notary mechanism and multi signature notary mechanism lies in the different signature methods. It adopts the idea of multi-party computing (MPC). MPC [5] refers to a group of participants who do not trust each other. While protecting personal privacy, they can also carry out collaborative computing. Its security is higher and its implementation is more complex. The distributed signature notary mechanism generates a unique key based on the password, splits the key (no one in the notary group will have the complete key) into multiple fragments (processed ciphertext) and distributes it to the randomly selected notary (even if all notaries put the fragments together, they cannot know the complete key), After allowing

a certain proportion of notaries to jointly sign, they can piece together a complete key, so as to complete a more decentralized "data collection and verification" process. The distributed signature notary mechanism comprehensively ensures the security of the key. This method is more flexible and secure. When a few nodes are attacked or various errors occur, it will not affect the whole system.

2.2 Side Chain/Relay

Side chain is a new type of blockchain based on anchoring a token on the original chain. For example, Ethereum can become the side chain of bitcoin, and bitcoin is the main chain of Ethereum. Under this mechanism, the main chain does not know the existence of the side chain, but the side chain knows the existence of the main chain, that is, the side chain can read the main chain. Side chain is a concept relative to the main chain. Blockstream's formal definition of "side chain" is "side chain is a blockchain that verifies data from other blockchains" [16]. When the expansion of the main chain encounters difficulties, the value assets on the main chain can be transferred to the side chain for trading, which enhances the expansibility of the main chain. In the current discussion, most of the side chains still refer to the anchored side chain mentioned by blockstream [1]. The anchored side chain supports the circulation and exchange of value assets between the main chain and the side chain. Bidirectional anchoring technology can be realized through the following modes: single hosting mode, alliance mode, SPV mode, drive chain mode and hybrid design [12].

The relay mode is suitable for linking two heterogeneous or isomorphic blockchains and is a more direct way to realize the interoperability of blockchains [13]. Both side chain and relay are the most commonly used cross chain modes, and the information on the original chain needs to be collected in the implementation process. Compared with the side chain, the relay is more flexible. The "middleman" only acts as the data collector. After the target chain receives the data from the sending chain, the receiving chain verifies it by itself to complete the transaction confirmation. The way of self verification varies according to the system structure. For example, BTC relay depends on SPV certification, Cosmos also depends on the number of signatures of verification nodes, etc.

2.3 Hash Locking

The hash function has the characteristics of unidirectionality and low collision, and hash locking [11] is a basic framework for cross-chain atomic transactions realized by using the inherent characteristics of the hash function combined with the characteristics of blockchain transactions that can be executed on a delayed basis. Assuming that account A on chain X wants to exchange assets with account B on chain Y, the hash locking process is as follows:

a) *A creates a random string s and calculates its hash value H = hash (s).*
b) *A sends the calculated hash value H to B.*

c) *A locks the assets it is preparing to exchange on the X chain and sets a relatively long time T1 (T1 can be highly expressed by a future blockchain), And set the conditions for acquiring the asset: if B can provide s in step a) within T1 time, it can obtain the asset locked by A on the X chain.*
d) *B observes that some assets are locked in A contract. Then B locks the assets ready to participate in the exchange on the Y chain and sets a relatively short time T2. B also sets the corresponding acquisition conditions: if A can provide s in step 1) within T2, A can obtain the assets locked by B on the Y chain.*
e) *A sends the string s initially generated by itself to B to obtain the asset locked by B on the Y chain.*
f) *B obtains the value s sent by A in step e) and sends it to A to obtain the assets locked by A on the X chain.*

In the above hash locking transaction, A has the initiative and is the more advantageous party. Therefore, cross chain hash locking is usually combined with "state channel" to make the transaction faster, so as to avoid the above A advantage problem.

2.4 Distributed Private Key Control

Distributed private key control [2], as its name suggests, is to use distributed nodes to control the private keys of various assets in the blockchain system, separate the use right and ownership of digital assets, so that the control right of assets on the chain can be safely transferred to the decentralized system, and map the assets on the original chain to cross chains, Realize asset circulation and value transfer between different blockchain systems. In order to ensure that the original chain assets can still trade and circulate with each other across the chain, the operation of realizing and releasing distributed control management is called lock in and lock out. Lock in is to manage the control right of digital assets through the key. The user and the decentralized network jointly take charge of the private key. There is no third party holding the private key. When unlocked, the control of digital assets is returned to the owner. The distributed private key control is similar to the notary mechanism, but in the distributed private key control technology, users and decentralized networks jointly have the right to control assets, avoiding the risk of centralization. Because the distributed private key control technology does not change the characteristics of the original chain, the cross chain needs to be developed according to the characteristics of the original chain, which also leads to the disadvantages of difficult development and small scope of application.

2.5 Notary+Side Chain Hybrid Technology

Based on the existing cross chain technology, some researchers combine the characteristics of simple and easy implementation of notary mechanism with the characteristics of fast and efficient side chain technology, and put forward the notary+side chain hybrid cross chain technology. This technology realizes value cross chain through notary mechanism, communicates between blockchains through side chain technology, supports cross chain asset interaction, cross chain contract and asset mortgage, and avoids centralized control by distributed nodes. It is the simplest way for chain to chain interoperability.

This technology also has some shortcomings, such as side chain technology is difficult to implement, and the distributed deployment of nodes can not be completely decentralized. At present, ether universe is the first in the world to adopt notary mechanism+side chain hybrid technology to realize EOS based on the 3rd generation blockchain platform The cross chain service platform built by IO is a set of completely innovative cross chain interaction technology solutions [7].

3 Notary Group Election

The notary mechanism introduces a person who is trusted by both parties as an intermediary, i.e. a notary, between two parties who do not trust each other. In the cross-chain transaction process of the notary mechanism, the notary only needs to verify whether the transaction information is consistent and legitimate, and does not need to verify the details of the transaction [15]. Compared with other cross-chain technologies, the biggest advantage of cross-chain mechanism based on notary group is that it is faster to process and easier to implement without complicated consensus mechanism.

Notary group mechanism cross-chain transactions require the honesty of most notaries, so the quality of the selected notary nodes is crucial to the success of the transaction. The existing notary groups are usually selected randomly, and if there are more malicious nodes in the randomly selected notary groups, it is more likely to lead to transaction failure. The web ranking algorithm PageRank [14] is introduced into the notary election process, and the average trust vote score among nodes is used as the base reputation value of nodes, and the dynamic joining and quitting of nodes in the notary group is realized through the change of reputation value, so that the trust problem of cross-chain users can be converted into the trust problem of the notary group.

3.1 Trust Score Calculation

The reputation value reflects the contribution of a notary in the notary group, as well as the loyalty and credibility of the notary node. The reputation value will change dynamically with the processing efficiency and transaction success rate of the node participating in the cross chain transaction of the notary group. When there is a transaction request, the system selects a certain number of notary representatives from the notary nodes with high reputation among notaries to form a notary group.

Each notary can define the weight of transaction processing efficiency and transaction success rate, then calculate the trust ranking according to the transaction processing efficiency and transaction success rate, and finally vote for the notary node he trusts.

The transaction success rate is an evaluation mechanism for the loyalty and credibility of nodes, which is expressed by formula (1).

$$\text{success}_{\text{A}->\text{B}} = \text{weight}_{\text{A}->\text{success}} \times \frac{Txs_B}{Tx_B} \tag{1}$$

Among them, $\text{success}_{\text{A->B}}$ represents the evaluation of notary node a on the success rate of node B's participation in the transaction, $\text{weight}_{\text{A->success}}$ represents the weight of notary node a on the success rate, Txs_{B} represents the number of successful transactions

participated by notary node B, and Tx_B represents the total number of transactions participated by notary node B.

Transaction efficiency refers to the processing speed of the public witness node when acting as the notary representative. It is another evaluation mechanism for the node, which is expressed by formula (2).

$$effic_{A->B} = weight_{A->effic} \times \frac{Txs_B}{T_B} \times \eta \tag{2}$$

Among them, $effic_{A->B}$ represents the evaluation of notary node a on the transaction efficiency of node B, $weight_{A->effic}$ represents the weight of notary node a on the efficiency evaluation, Txs_B represents the number of successful transactions in which notary node B participates, T_B represents the total duration of successful transactions in which notary node participates, and parameter η is used to adjust the value of $\frac{Txs_B}{T_B}$ to make it between [0, 1], Ensure that the transaction success rate is in the same range.

The trust score of notary node a to node B is:

$$R_{A->B} = effic_{A->B} + success_{A->B} \tag{3}$$

According to formula (3), notary node a can calculate the trust score of all nodes according to its own weight distribution method, and then node a will vote for the notary node with the highest trust score according to the representative size of the notary group required by the exchange. Other nodes choose their trusted nodes and vote in the same way.

3.2 Reputation Value Calculation of Improved PageRank Algorithm

PageRank, or web page ranking, also known as web page level, is a link analysis algorithm proposed by Google founders Larry Page and Sergey Brin when they built an early search system prototype in 1997 [9]. PageRank evaluates the importance of web pages according to the number of web pages entering the chain and the quality of web pages entering the chain. For an Internet web page, its importance is calculated based on the following two assumptions:

1) *Quantity assumption: in the Web graph model, if a page node receives more incoming links from other pages, the more important the page is.*
2) *Quality assumption: the quality of links to pages is usually different. High quality pages will pass more weight to other pages through links. Therefore, the more high-quality pages point to the page, the more important the page is.*

Using the above two assumptions, PageRank algorithm gives each page an initial value representing the importance, and then recursively calculates the importance score of each page according to PageRank algorithm until the score is stable. However, due to the existence of isolated web pages with out chain of 0, the PageRank algorithm needs to be modified. The modified PageRank algorithm introduces the damping coefficient d, which is usually taken as $d = 0.85$. The modified PageRank formula is shown in (4).

$$PR(A) = \frac{1-d}{N} + d \times \sum_{i \in C_A} \frac{PR(i)}{L(i)} \tag{4}$$

Where N represents the total number of pages, C_A represents all page collections, PR(i) represents the importance of pages, and L(i) represents the total number of pages chained out by page i. Using the above formula (4) for cyclic iterative calculation, it is finally obtained that the PR value of each page will tend to be stable. Finally, the importance of all pages will be sorted according to the stable PR value.

In formula (4), the traditional PageRank algorithm has the following shortcomings:

- For all nodes, the same part (1 − d)/N is added in the process of reputation value calculation, which can not well reflect the different initial states between different nodes.
- The traditional PageRank algorithm evenly distributes the reputation value of nodes to all trusted nodes, which affects the ranking quality of reputation value to a certain extent.
- The newly added nodes usually rank lower because they participate in fewer transactions. The probability of being selected as a notary is very small, and they will never have the opportunity to participate in the transaction as a notary.

In view of the problems existing in the traditional PageRank algorithm, this paper proposes the following improvement methods:

- In the improved algorithm, the result of trust voting between nodes is introduced, and the average score of trust voting between nodes Rave-i is taken as the initial reputation value of nodes, which fully considers the trust relationship between nodes.
- According to the initial voting score of the node, the reputation value of the node is allocated to the trusted nodes in proportion.
- Adjust the damping coefficient d to adjust the reputation value of the new node, so as to ensure that the new node also has the opportunity to become a notary.

Calculate the reputation value of notary nodes based on the improved PageRank algorithm, as shown in formula (5). Using the average value of the trust score as the initial reputation value of each node reduces the initial value of the reputation value of malicious nodes, which can effectively avoid malicious nodes from entering the notary group.

$$\mathrm{PR(i)} = \mathrm{R_{ave\text{-}i}} + \mathrm{d} \times \sum_{j \in C_i} \left(\mathrm{PR(j)} \times P_{i,j}\right) \tag{5}$$

Where PR(i) represents the reputation value of notary node i and $R_{ave\text{-}i}$ represents the average trust score of notary group node i. The calculation method is as shown in formula (6). d is the damping coefficient in PageRank. For newly added nodes, the damping coefficient is taken as 1. j is the node that cast the trust vote for notary node i, C_i is the set of all nodes that cast the trust vote for node i, and $P_{i,j}$ is the proportion of the initial score of node i in the total score of node j. the calculation method is as follows (7).

$$\mathrm{R_{ave\text{-}i}} = \frac{\sum_{jQ\&i \notin Q} R_{j \to i}}{N - 1} \tag{6}$$

Where $R_{ave\text{-}i}$ represents the average trust score of node i of notary group, j belongs to any notary node, Q is the set of all notary nodes except node i, $R_{j->i}$ represents the trust score given by notary node j to node i, and N is the number of all nodes.

$$P_{i,j} = \frac{R_{j \to i}}{\sum_{k \in M} R_{j \to k}} \tag{7}$$

Where, $P_{i,j}$ is the proportion of the initial score of node i in the total score of node j, $R_{j->i}$ is the trust score of notary node j to node i calculated according to formula (3), and M is all node sets of node j voting. Due to the attack behavior of malicious nodes, if a malicious node A only votes for another malicious node B, that is, there is only one element in set M, this will rapidly increase the reputation score of malicious node B. In order to prevent this situation, it is stipulated that when the value of $P_{i,j}$ calculated according to the formula is greater than 1/3, the value of $P_{i,j}$ is 1/3.

4 Experimental Analysis

In order to more objectively verify the effectiveness of the dynamic notary group election model based on reputation value, the following experimental analysis is carried out.

Eight notary nodes are selected in this experiment, and the parameter configuration of each node is shown in Table 1.

The table lists the historical transaction information with each experimental node. T_{num} represents the total number of times that the node has participated in the transaction, T_{succ} represents the number of successful transactions that the node has participated in, T_{time} represents the total time of successful transactions that the node has participated in, w_{effic} represents the efficiency weight set by the node, and $w_{success}$ represents the weight of the successful transaction rate set by the node. In order to prevent malicious node damage, the sum of the two weight values is required to be a fixed value, which is set to 5 here.

According to the algorithm in Sect. 3, Part A (where the adjustment parameter η is 0.1), each node calculates the trust scores of other nodes, as shown in Table 2.

Table 1. Parameter configuration of experimental nodes

node	T_{num}	T_{succ}	T_{time}	w_{effic}	w_{succ}	remarks
A	12	10	2.80 s	3	2	Common
B	5	1	0.30 s	2	3	Malicious
C	8	8	2.50 s	2.5	2.5	Common
D	9	9	2.70 s	3.5	1.5	Common
E	16	15	3.00 s	4	1	Common
F	4	1	0.280	3	2	Malicious
G	10	9	2.40 s	1	4	Common
H	0	0	0	2.5	2.5	New

Table 2. Calculation of trust score between nodes

i, j	A	B	C	D	E	F	G	H
A	0	1.4000	2.9600	3.0000	3.3714	1.5714	2.9250	2.0000
B	3.2142	0	3.6400	3.6667	3.8071	1.4643	3.4500	3.0000
C	2.9761	1.3333	0	3.3333	3.5893	1.5179	3.1875	2.5000
D	2.4999	1.4667	2.6200	0	3.1536	1.6250	2.6625	1.5000
E	2.2619	1.5333	2.2800	2.3333	0	1.6786	2.4000	1.0000
F	2.7380	1.4000	2.9600	3.0000	3.3714	0	2.9250	2.0000
G	3.6903	1.1333	4.3200	4.3333	4.2428	1.3571	0	4.0000
H	2.9761	1.3333	3.3000	3.3333	3.5893	1.5179	3.1875	0
Ave	2.9081	1.3714	3.1543	3.2857	3.5893	1.5332	2.9625	16.0000

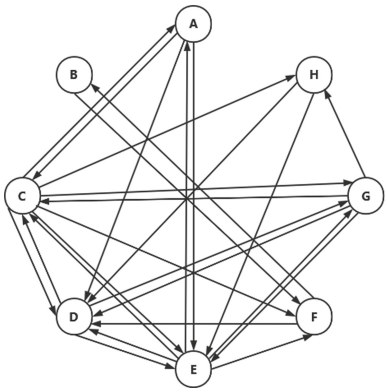

Fig. 1. Directed graph of trust relationship between nodes

The average trust score is $R_{ave\text{-}i}$ in Eq. (6), and (i, j) represents the reputation value of node j calculated by node i. As shown in Table 3, the first behavior node A calculates the trust values of other nodes according to its own weight distribution. Node A can vote for the top ranked nodes as needed. Due to the attack behavior of malicious nodes, when voting, malicious nodes do not vote for nodes with high trust scores according to the rules, but choose ordinary nodes or malicious nodes with low scores. Other ordinary nodes vote for their trusted nodes according to the rule of trust score from high to bottom. The directed graph of trust voting of each node is obtained from Table 3, as shown in Fig. 1.

Where A—>C shows that node A trusts node C and votes for node C. The damping coefficient in the improved PageRank algorithm selected in this experiment is $d = 0.8$. The reputation value PR(i) of each node is iteratively calculated according to formula (6). When the difference between the reputation values calculated by all nodes before

Table 3. Dynamic calculation of node reputation value

times	PR(A)	PR(B)	PR(C)	PR(D)	PR(E)	PR(F)	PR(G)	PR(H)
0	2.90810	1.37140	3.15430	3.28570	3.58930	1.53320	2.96250	2.28570
1	3.94011	1.76167	6.09632	6.94545	7.15977	2.56288	4.89150	3.66563
2	4.93947	2.02377	8.37646	9.43497	9.78050	3.31355	6.87999	4.69396
3	5.68980	2.21485	10.21527	11.49875	11.89125	3.86661	8.30787	5.64401
…	…	…	…	…	…	…	…	…
44	8.60493	2.89291	17.17900	19.31949	20.01003	5.97738	13.90888	9.11073
45	8.60498	2.89292	17.17910	19.31961	20.01015	5.97741	13.90897	911078
46	8.60501	2.89292	17.17919	19.31971	20.01025	5.97744	13.90903	9.11082

and after is less than 0.0001, we believe that the reputation value has reached stable convergence.

The average trust score of each node represents their initial reputation value. The reputation value of each node is calculated iteratively. The calculation process of reputation value of each node is shown in Table 3.

The calculation results show that when the iteration reaches the 46th time, the difference between the reputation value of each node and the reputation value calculated at the 45th time is not greater than the parameter 0.0001 set by us. The reputation value iteration calculation ends and the final reputation value of each node is obtained. Finally, all nodes are sorted according to the size of reputation value. According to the result, the nodes are sorted as: EDCGHAFB. The higher the ranking, the higher the credibility and loyalty of the node, and the greater the probability of being selected as a notary representative. In each transaction, select the required notary representatives from the new reputation value ranking to form the notary group of this transaction.

5 Conclusion

By improving the form of PageRank algorithm and adding the concept of reputation value, this paper transforms the original inter-chain trust problem into the trust problem among nodes, reduces the risk of centralization of notary mechanism, and improves the success rate of cross-chain transactions. The article extends the mechanism of randomly selected notaries to dynamic notary group election based on reputation value, which reduces the probability of malicious nodes being selected as notary representatives and is more relevant to practical applications. Through experiments, the reliability of the node reputation values calculated based on the improved PageRank improvement algorithm is verified. In addition the effect of different values of damping coefficients on the final reputation value results can be further explored.

References

1. BACK A, CORALLO M, DASHJR L, et al. Enabling Blockchain Innovations with Pegged Sidechains[EB/OL]. http://www.bubifans.com/ueditor/php/upload/file/20181015/1539599182599463.pdf, 2019-4-17.
2. Chan, and A. C.-F., "Distributed Private Key Generation for Identity Based Cryptosystems in Ad Hoc Networks." Wireless Communications Letters, IEEE (2012).
3. Di Yang, Chengnian Long, Han Xu and Shaoliang Peng. 2020. A Review on Scalability of Blockchain. In Proceedings of the 2020 The 2nd International Conference on Blockchain Technology (ICBCT'20). Association for Computing Machinery, New York, NY, USA, 1–6. DOI: https://doi.org/10.1145/3390566.3391665.
4. E. J. Scheid, P. Kiechl, M. Franco, B. Rodrigues, C. Killer and B. Stiller, "Security and Standardization of a Notary-based Blockchain Interoperability API," 2021 Third International Conference on Blockchain Computing and Applications (BCCA), 2021, pp. 42–48.
5. Goldreich, O. , and A. Warning . "Secure Multi-Party Computation." Information Security & Communications Privacy (2014).
6. Guo, H. , et al. "Attribute-based Multi-Signature and Encryption for EHR Management: A Blockchain-based Solution." IEEE (2020).
7. Kim, Henry M. ,and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance." International Journal of Intelligent Systems in Accounting, Finance & Management (2018).
8. Li F, Li ZR and Zhao H. Research on the progress in cross-chain technology of blockchains. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1649−1660.
9. Lt, A ,A.Jfv and B. Gy, "An algorithm for ranking the nodes of multiplex networks with data based on the PageRank concept." Applied Mathematics and Computation (2021).
10. Miraz, M. H, and D. C. Donald, "Atomic Cross-Chain Swaps: Development, Trajectory and Potential of Non-Monetary Digital Token Swap Facilities." Social Science Electronic Publishing (2019).
11. Mohanty S K, Tripathy S , n-HTLC: Neo hashed time-Lock commitment to defend against wormhole attack in payment channel networks - ScienceDirect[J]. Computers & Security, 2021, 106.
12. Oleksii Konashevych and Marta Poblet. 2019. Blockchain Anchoring of Public Registries: Options and Challenges. In Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance (ICEGOV2019). Association for Computing Machinery, New York, NY, USA, 317–323. DOI: https://doi.org/10.1145/3326365.3326406.
13. P. Frauenthaler,M.Sigwart,C.Spanring and S.Schulte, "Testimonium: A Cost-Efficient Blockchain Relay." (2020).
14. S. Kamvar ,T. Haveliwala and G. Golub, "Adaptive methods for the computation of PageRank." Linear Algebra and its Applications 386.1(2004):51–65.
15. Schwartz E. A payment protocol of the web, for the web: or, finally enabling web micropayments with the interledger protocol[C]//In Proceedings of the 25th International Conference Companion on World Wide Web (WWW'16 Companion). Republic and Canton of Geneva: International World Wide Web Conferences Steering Committee, 2016, 279–280.
16. Vitalik Buterin. Chain Interoperability[EB/OL]. https://static1.Squarespace/com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdfi, 2016-9-9/2019-4-7.