electronics

Article

Three-Stage Cross-Chain Protocol Based on Notary Group

Longfei Chen [1,2,*], Zhongyuan Yao [1,2], Xueming Si [1,2] and Qian Zhang [1]

[1] Frontier Information Technology Research Institute, Zhongyuan University of Technology, Zhengzhou 450007, China; yaozhongyuan@zut.edu.cn (Z.Y.); 9773@zut.edu.cn (X.S.); 6382@zut.edu.cn (Q.Z.)
[2] Henan International Joint Laboratory of Blockchain and Data Sharing, Zhengzhou 450007, China
* Correspondence: 2021016570@zut.edu.cn

Abstract: With the continuous development of blockchain technology and economy, blockchain applications have been well developed in multiple key areas. The demand for interoperability between different blockchains is also increasing. Cross-chain protocol has become a major approach to solve cross-chain problems by defining a series of cross-chain processes and standards. In response to the problems of long transaction time, high transaction costs, and high degree of centralization in most cross-chain protocols, this paper proposes a three-stage cross-chain protocol based on transaction notary groups and verification notary groups. Without increasing transaction costs and transaction time, the centralization problem of notary mechanism cross-chain technology is solved, realizing secure and fast interaction between different blockchains. Experimental results show that as long as malicious nodes in the notary group do not exceed one-third, the three-stage cross-chain protocol can effectively ensure the security of cross-chain transactions and solve the centralization problem.

Keywords: interoperability; blockchain; cross-chain; cross-chain protocol; notary group

Citation: Chen, L.; Yao, Z.; Si, X.; Zhang, Q. Three-Stage Cross-Chain Protocol Based on Notary Group. *Electronics* **2023**, *12*, 2804. https://doi.org/10.3390/electronics12132804

Academic Editor: Mehdi Sookhak

Received: 30 May 2023
Revised: 17 June 2023
Accepted: 22 June 2023
Published: 25 June 2023

1. Introduction

In 2022, the global blockchain technology market reached 11.14 billion [1] and is expected to grow from 17.57 billion in 2023 to 469.49 billion in 2030, of which the financial sector [2] accounted for 31.5% as the largest application field. In addition to the financial sector, blockchain technology is also widely used in other fields such as supply chain [3], intelligent healthcare [4], Internet of Things [5], and energy trading [6]. The blockchain application and underlying technology platform are currently in a state of great diversity, but most mainstream blockchain applications still consist of independent, vertical closed systems. There is a lack of a unified interconnection mechanism between chains which leads to the phenomenon of 'value islands' between systems. This greatly limits the flow of digital value on the blockchain. Blockchain cross-chain technology can break the 'value island' between different blockchain systems and achieve interoperability and multi-integration between chains, which has become the focus of the current blockchain technology research field.

With the development of cross-chain technology, cross-chain protocols have become an effective way to solve the problem of cross-chain communication in blockchain [7]. Cross-chain protocols can be classified into three categories based on the underlying cross-chain mechanism: cross-chain protocols based on hash locking mechanisms [8], cross-chain protocols based on sidechain/relay mechanisms [9,10], and cross-chain protocols based on notary mechanisms [11]. While these three categories of cross-chain protocols solve specific challenges, they also face many shortcomings. Cross-chain protocols based on the hash-locking mechanism have long overall transaction times and limited application scenarios. For example, Komodo's atomic swap protocol can exchange small transactions through simple and fast steps [12]. However, for large transactions, users still need to wait for a long time, especially when many users are using the protocol simultaneously, which may result in network congestion and delays. Cross-chain protocols based on the sidechain/relay mechanism have good scalability but are difficult to implement. For example, IBC (Cosmos) [13], XCMP (Polkadot) [14], and IBTP (BitXHub) [15] support access to different heterogeneous chains but have high transaction costs, implementation difficulty, and require a lot of resources to support. Cross-chain protocols based on the notary mechanism have the advantages of fast transaction speed and easy implementation, but they rely too much on the honesty of a single notary node, resulting in high centralization. Therefore, if the centralization problem in the current notary mechanism can be solved and the dependence on a single trusted node can be eliminated, it may become possible to achieve higher efficiency and better cost-effectiveness in cross-chain interoperability.

This article proposes a three-stage cross-chain protocol based on a group of notary nodes, aiming to solve the centralization problem in the existing notary mechanism. The protocol adopts an improved PageRank ranking algorithm [16] to improve the notary election strategy, evaluate each node's performance from multiple dimensions, and comprehensively elect a transaction notary group responsible for transaction work and a verification notary group responsible for verification and supervision work. At the same time, the protocol meticulously designs the entire cross-chain transaction into three stages: pre- transaction stage, transaction stage, and confirmation stage, and uses a decentralized threshold digital signature algorithm [17] to be responsible for data authentication and security.

The main contributions and innovations of this paper are as follows:

- Based on an improved PageRank notary ranking algorithm, the transaction notary group and verification notary group are elected based on parameters such as the node's historical transaction records, message response time, and mortgage margin size to complete cross-chain transactions. On the one hand, it increases the probability of electing honest nodes, while ensuring the randomness of the election.
- Decentralized threshold signature algorithm is used to ensure the robustness and privacy of the transaction notary group and verification notary group in the signing and verification process.
- The protocol divides the entire transaction process into three stages: pre-transaction stage, formal transaction stage, and confirmation stage. The verification notary group is responsible for monitoring and verifying the entire transaction, while the transaction notary group is responsible for accurate execution of the transaction process, meeting the consistency and atomicity requirements of cross-chain transactions.
- The verification and monitoring work is separated from the specific transaction work throughout the cross-chain transaction process, which ensures the transaction speed of the system while effectively improving the security of the entire system.

The structure of this paper is as follows: Section 1, Introduction, introduces the back ground information of blockchain cross-chain technology; Section 2, Related Work, discusses and compares cross-chain protocols in the field of blockchain cross-chain over the past three years; Section 3, Preliminary Knowledge, introduces the improved PageRank ranking algorithm and the decentralized threshold digital signature algorithm; Section 4, Methodology, introduces the model of the three-phase cross-chain protocol and the three phases of protocol cross-chain transactions; Section 5, Performance Analysis, conducts security, experimental, and comparative analysis of the three-stage cross-chain protocol; Section 6, Conclusions.

2. Related Work

In recent years, with the significant increase of scholars' research in the field of blockchain interoperability and the continuous improvement of cross-chain technology, a series of cross-chain protocols have been proposed to provide cross-chain standards and processes. Cross-chain protocols rely on cross-chain mechanisms to define a series of communication data formats, interface specifications, and cross-chain processes to achieve communication and interaction between homogeneous or heterogeneous blockchains and achieve cross-chain transaction synchronization. This article summarizes the relevant literature on cross-chain protocols over the past three years. Cross-chain protocols based on hash locking require that when the sender transfers funds, the receiver can accept the funds within a specific time to ensure the atomicity of cross-chain asset exchange. Although this type of cross-chain protocol optimizes the trading environment and enhances transaction security, it often faces drawbacks such as high transaction costs, long transaction times, and limited application scenarios [18–24]. Therefore, it is not suitable for large-scale applications. For example, literature [18] creates a new cryptographic primitive AVTC (Attribute Verifiable Timed Commitment) to execute the transaction process of atomic exchange, reducing the time for both parties to complete the transaction, but increasing the transaction costs for both parties; literature [20] improves the security of transactions for both parties through insurance fees, but also increases the transaction costs for both parties; literature [24] requires seamless exchange of assets between different blockchains in a secure network environment, which cannot be achieved in a normal environment.

In cross-chain protocols based on sidechain/relay mechanism, a series of interaction standards between parallel chains and relay chains are defined, including interaction ports, Certification models, transaction methods, routing information, and other components, in order to achieve trusted interaction between different blockchains. This approach has rich functionality and broad application scenarios [25–29], but the downside is that the overall network communication overhead is high and most remain in the experimental stage, with some distance from large-scale usage. For example, literature [27] has strong scalability, but the effectiveness of the protocol model needs further verification.; literature [28] supports homogenous and heterogeneous chain transactions, with portability and no restriction on cryptocurrency type, but the transaction costs are high, and it cannot currently be implemented on the Ethereum mainnet.

Cross-chain protocols based on notary mechanisms are in conflict with the decentralized characteristics of blockchain technology. Therefore, this category of cross-chain protocols mainly focuses on optimizing and improving cross-chain technology based on notary mechanisms [30–33], reducing reliance on individual nodes or individual blockchains, and making the entire interaction network more secure and efficient. For example, literature [30] collects data and converts it into a unified data format through a committee composed of multiple notary nodes, achieving information exchange between different blockchains; literature [33] is responsible for locking and redeeming assets through a third-party insurance library. In summary, trusted third-party notaries play the role of both validator and regulator in the cross-chain interaction process. Therefore, the notary mechanism has the advantages of fast transaction speed and low implementation difficulty. If the traditional notary mechanism can be broken through, the mode of electing a single node to be responsible for the entire cross-chain transaction process can be canceled and the dependence on a single node can be eliminated, which can make the entire cross-chain protocol have the advantages of fast transaction speed and easy implementation, while reducing centralization risk.

3. Preliminary Knowledge

3.1. PageRank Notary Ranking Algorithm

PageRank ranking algorithm is a method used by Google to evaluate the importance of web pages. It recursively calculates the link relationships between web pages, generates a web page weight vector, and sorts the web pages based on the size of the weight vector. The higher the PageRank value, the more important the web page is. The protocol mainly improves the election strategy by introducing parameters such as the historical transaction records of nodes, message response time, the size of the notary's pledged margin, and evaluations from other notary nodes. The corresponding weights are then assigned according to their importance. Table 1 lists the properties of each parameter.

Table 1. Parameter attribute list information.

Parameter Name	Weight	Specific Information
$\frac{PR(n)}{L(n)}$	0.5	Evaluation value of node n towards other nodes
α	0.2	Average response time
β	0.2	Percentage of margin
γ	0.1	Historical completed trading volume

$\frac{PR(n)}{L(n)}$ represents the evaluation value of node n towards other nodes, specifically, whether there exists a trust relationship between them. This is the foundation of trust for the entire notary group. If two nodes have a trust relationship, they can evaluate each other and assign corresponding evaluation values. This trust relationship can be obtained through joint participation in completing a transaction. The more such relationships a node has, the higher its credit value and the more trustworthy it is. Therefore, this parameter occupies half of the weight; The faster a node responds to messages and the more various forms of information it forwards, the stronger its ability to process transactions. The indicator α of the average response time reflects this ability. The higher the value of α, the better the performance of the node in handling transactions; When each node joins the notary group, it will transfer a deposit to the margin pool. The higher the deposit, the greater the cost the node has to bear after misconduct. As a result, the probability of misconduct is greatly reduced. Therefore, the more deposit is pledged, the higher the margin ratio indicator β; The more transactions a node participates in and completes, the larger the historical completed trading volume indicator γ. To balance the number of transactions of newly added nodes, the weight of this part is 0.1.

Here are the specific calculation steps: First, N is the number of notary nodes in the notary group, and m represents the participants. The average response time indicator α of node $m_i(i = 1,2...N)$ is inversely proportional to the average response time t of the node. The shorter the average response time t, the larger the value of α. The total value of the average response time of all notary nodes is $T = \sum_{i=1}^{n} \frac{1}{t_i}$, then the final average response time indicator of node m_i is $\alpha = 0.2(\frac{1}{t_i T})$; Next, the total amount of deposit for all notary nodes in the notary group is calculated as $D = \sum_{i=1}^{n} d_i$, and the deposit ratio indicator of node m_i is $\beta = 0.2(\frac{d_i}{D})$; Finally, the total number of historical transactions of all notary nodes is calculated as $H = \sum_{i=1}^{n} h_i$, and the historical completed transaction volume indicator of node m_i is $\gamma = 0.1(\frac{h_i}{H})$. The improved PageRank algorithm is as follows:

$$R(m) = \frac{1-d}{N} + d \times (0.5 \sum_{n \in V} \frac{PR(n)}{L(n)} + \alpha + \beta + \gamma).$$

$PR(m)$ represents the credit value that node m ultimately obtains; d is the damping coefficient, which is defined as 0.85 here; N represents the number of nodes in the notary group; V represents the incoming set of nodes m; $PR(n)$ represents the credit value of node n; $L(n)$ represents the number of nodes that node n evaluates.

3.2. Decentralized Threshold Digital Signature Algorithm

In threshold digital signature, the key is allocated to multiple people for management by using threshold technology, so that k or more participants are required to participate in signing for it to be effective, thus ensuring the security of the signature. This protocol adopts a decentralized threshold digital signature algorithm, which uses interpolation polynomials to split, distribute, and recover the key, allowing each participant to complete the digital signature work without revealing their key information. The signature algorithm is as follows: In the initialization phase, assume that q is a large prime number and n is the number of participants. Each participant $P_i(i = 1,2...n)$ has a key $s_i \epsilon GF(q)$, where $GF(q)$ is a finite field with characteristic prime number q. All participants share a master key $s = \sum_{i=1}^{n} s_i$.

In the key distribution phase, each participant P_i picks a $k-1$ degree polynomial $f_i(x)$ such that $s_i = f_i(0)$. P_i computes $m_{ij} = f_i(j)$, $j = 1, 2 \ldots n$ and sends the resulting security key m_{ij} to the other participants P_j. Finally, participant P_i computes $m_i = \sum_{i=1}^{n} m_{ji}$ after receiving all messages from the other participants. In the key verification phase, all participants P_i randomly select a set of n-dimensional vectors on $GF(q)$ denoted by $(a_1, a_2 \ldots a_n)$. Each participant P_i publishes $v_i = \sum_{j=1}^{n} a_j m_{ji}$, and all participants jointly compute the interpolation polynomial $f_v(x)$ passing through all the points (i, v_i), $i = 1, 2 \ldots n$. If the polynomial $f_v(x)$ is a $k-1$ degree polynomial, then the sub-keys of all participants are valid; otherwise, there is cheating by one or more participants. In the key recovery phase, any k participants, it may be assumed that $P_1, P_2 \ldots P_k$ can be used to recover master key s by a LaGrange interpolation formula. The specific algorithm is as follows:

$$s = \sum_{i=1}^{k} m_i \sum_{j=1, j \neq i}^{k} \frac{-j}{i-j}.$$

4. Methodology

4.1. System Architecture

As shown in Figure 1, the main body of the three-stage cross-chain protocol consists of three parts: the origination chain, the target chain, and the notary group. The origination chain is the blockchain on which the initiator initiates the cross-chain transaction, the target chain is the blockchain where the recipient of the cross-chain transaction is located, and the notary group is a cluster of notary nodes composed of many nodes. The transaction notary group and the validation notary group can be elected through the group of notary nodes to complete the cross-chain transaction, and each node in the notary group has accounts on both the origination chain and the target chain.

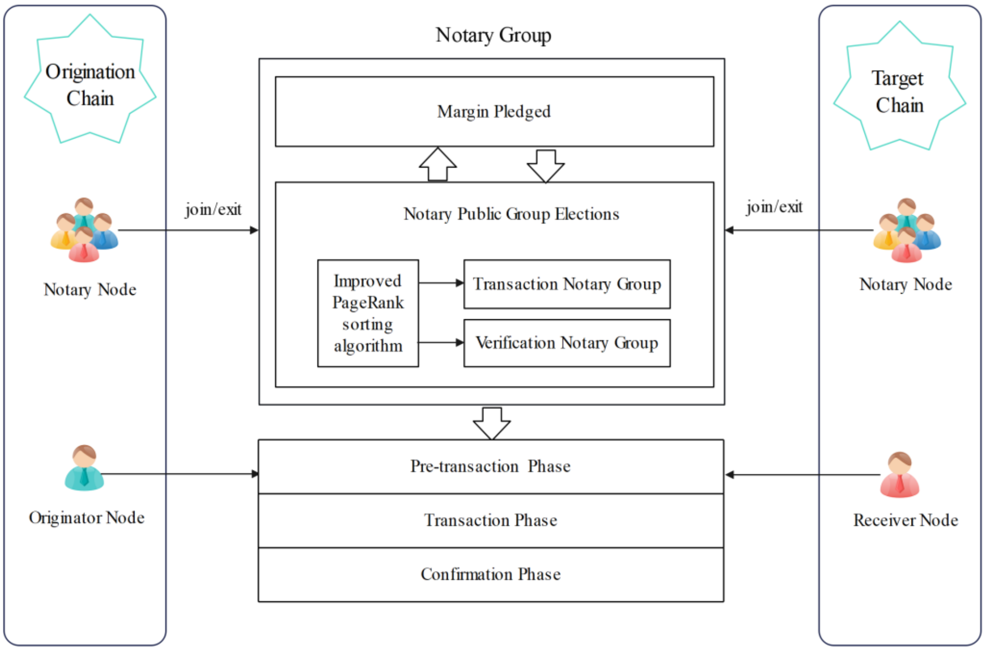

Figure 1. Three stage cross-chain protocol model.

4.1.1. Management of the Notary Group

The management of the notary group consists of three main parts: the join of the notary group, the exit of the notary group, and the election of the transaction and verification notary group. As shown in Figure 1, the notary group consists of two parts, the set of notary nodes and the margin pledged by the notary nodes. The set of notary nodes from which the transaction notary group and the verification notary group will be elected during the transaction process. The margin is a margin pledged by the node to join the notary group to prevent the current node from disruption and is returned to the node when it withdraws from the notary group.

1. Join the notary group;

Nodes applying to join the notary group must have accounts in both the originating chain and the target chain. The new node first needs to pay a certain margin to the notary group, specifically to the escrow accounts of the initiating chain and the receiving chain, respectively. Secondly, it needs to be verified by the members of the notary group. Once verified, they can join the notary group and their credit value will be $\frac{\boldsymbol{1-d}}{\boldsymbol{N}}$. The notary group is open to all nodes and the joining process is simple, any node that meets the requirements can join the notary group and participate in cross-chain transactions.

2. Exit from the notary group;

For a notary node to exit the notary group, it needs to apply to the group and be verified by other nodes. Once verified, the node can exit the transaction, and the margin pledged will be returned to the node within a specified time period. There are two types of notary group exits:

Normal exit: To exit the notary group, a member must complete all transactions and be verified by other members within the group. Once verified, the member can exit the notary group and reclaim the margin pledged.

Abnormal exit: If a notary node applies to exit the notary group while there are ongoing transactions, it cannot exit the group until all transactions are completed. Once the transactions are completed and verified by other nodes, the notary node can exit the notary group and reclaim its margin pledged. If a member exhibits malicious behavior, their margin pledged will be confiscated, and the member will be kicked out of the notary group. The malicious behavior will also be broadcasted, and the member will be permanently banned from joining any notary group.

3. Transaction and verification of the election of the notary group;

The improved PageRank algorithm is used to update the credit scores of existing notary nodes in the notary group within a certain period of time. Firstly, the notary group sends contract information to each notary node and broadcasts the system's temporary public key and address information. After receiving the signal, each notary node encrypted the evaluation data with the system public key and encrypted and signed it with its own private key, and then broadcast it to the network. The notary group collects the encrypted data from each node, decrypts them, and forms a trust relationship graph for this session. Secondly, using metrics such as average response time, historical transaction records, and margin ratios, the credit scores of each node during a certain period are calculated holistically. Finally, the transaction notary group and the verification notary group are randomly selected, with higher credit scores resulting in a greater chance of being selected.

4.1.2. The Three Stages of Cross-Chain Transaction

In the cross-chain transaction process, the protocol divides the transaction into three stages, namely the pre-transaction stage, transaction stage, and confirmation stage. Firstly, in the pre-transaction stage, the origination chain broadcasts the transaction form, confirms the transaction object, and elects the transaction notary group and the verification notary group as trusted third parties for this transaction. Secondly, in the transaction stage, the buyer and seller complete the cross-chain transaction through the workflow of the transaction notary group based on the protocol, including verifying billing data, locking and releasing assets, and so on. Finally, in the confirmation stage, the verification notary group is responsible for supervising and verifying the entire transaction, and after the transaction stage, it is responsible for the final confirmation of the transaction.

4.2. Three-Stages Cross-Chain Protocol

Based on the model above, this section describes in detail the specific transaction flow of the three-stage cross-chain protocol based on the notary group. To better demonstrate the principle of the three-stage cross-chain protocol, Table 2 uniformly shows the list of relevant attributes.

Table 2. List of protocol-related attributes.

Attribute Name	Identification
Originator Account	ID_S
Recipient Account	ID_R
Notary Group Accounts	ID_{NG}
Transaction the accounts of the notary group	ID_{TNG}
Verification the accounts of the notary group	ID_{VNG}
Signature of initiator	Sig_S
Signature of the recipient	Sig_R
Transaction of notary team signatures	Sig_{TNG}
Verification of notary team signatures	Sig_{VNG}
Related Form Information	TX

4.2.1. Pre-Transaction Stage

The pre-transaction stage prepares for the formal transaction stage. As shown in Figure 2 and Algorithm 1, the initiator initiates a cross-chain transaction request TX_1 and broadcasts it to the transaction network. The notary nodes in the notary group listen to the network information and initiate the form TX_2 to notify the receiver to process the cross-chain transaction. The recipient chooses whether to agree to this transaction according to the need and gives the transaction receipt TX_3. The notary group makes a judgment after obtaining the transaction receipt. If the receiver rejects the transaction, the notary group will forward the receipt TX_4 to directly notify the initiator and end the cross-chain transaction. If the receiver agrees to the transaction, the notary group will elect the transaction notary group TNG and the verification notary group VNG by the Improved PageRank sorting algorithm.

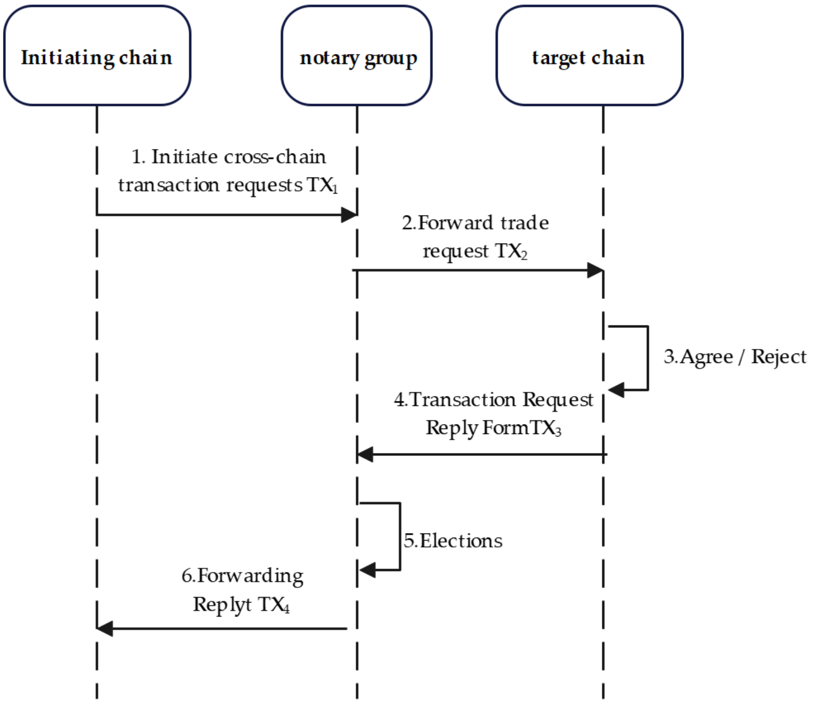
Initiating chain
notary group
target chain
1. Initiate cross-chain transaction requests TX_1
2.Forward trade request TX_2
3.Agree / Reject
4.Transaction Request Reply FormTX_3
5.Elections
6.Forwarding Replyt TX_4

Figure 2. Flow chart of pre-transaction stage.

The verification notary group VNG will be used as an example to explain the application of decentralized threshold key in the transaction process. After electing the transaction notary group, each node in the notary group generates a key $\boldsymbol{k_i}$, and together they form the master key $\boldsymbol{k = \sum_{i=1}^{n} k_i}$. Firstly, each node selects an $\boldsymbol{m - 1}$ degree polynomial $\boldsymbol{f_i(x)}$ and sets $\boldsymbol{k_i} = \boldsymbol{f_i(0)}$. At the same time, each node calculates $\boldsymbol{m_{ij} = f_i(j),\ j = 1, 2 \ldots n}$, and sends $\boldsymbol{m_{ij}}$ to other nodes in the notary group. Secondly, each node calculates $\boldsymbol{m_i = \sum_{i=1}^{n} m_{ji}}$ after receiving all information sent by other participants and prepares for signature verification and key recovery. Since these operations are all performed offline, they will not affect the overall transaction time of the cross-chain transaction. Lastly, the elected transaction notary group TNG and verification notary group VNG information will be sent to both parties, thus ending the pre-transaction stage and preparing for the formal transaction.

Algorithm 1. Pre-transaction stage algorithm

```
Input: $TX$; $ID_S$; $ID_R$; $ID_{NG}$; $Sig_S$; $Sig_R$
Output: $List_{TNG}$, $List_{VNG}$//The list of trading notary group and validate
notary group
function PREPAIRTRANSAction($TX$, $ID_S$, $ID_R$, $ID_{NG}$, $Sig_S$, $Sig_R$)
    S. LaunchTX$_1$($ID_S$, $Sig_S$)
    NG. LaunchTX$_2$($TX_1$, $ID_S$, $ID_R$)
R. LaunchTX$_3$($TX_2$, $ID_R$, $SIG_R$)
    if TX.CheckContent($TX_3$ == true) then
  $List_{NG}$←InsertList($ID_{NG}$)
        SelectTNG($List_{TNG}$, $List_{NG}$)
  SelectVNG($List_{VNG}$, $List_{NG}$) else
        SendTransaction ($TX_4$)
          break
 end if
 return $List_{TNG}$, $List_{VNG}$
 end function
```

4.2.2. Transaction Stage

The transaction stage is the official transaction stage. As shown in Figure 3 and Algorithm 2, the initiating party transfers the transaction funds to the account of the transaction notary group and sends the transaction credentials TX$_5$ to the account of the Verification notary group. The transaction notary group retransmissions the transaction request TX$_6$. After the receiver obtains the transfer information, it also transfers the funds into the account of the transaction notary group and sends the transaction certificate TX$_7$ to the verification notary group.

The verification notary group verifies the transaction certificates of both parties, and if there are no errors, it initiates a form for the transaction notary group to release the escrowed funds. At this time, the verification notary group needs to restore the main key for signature, which is $\boldsymbol{k = \sum_{i=1}^{k} m_i \sum_{j=1, j\neq i}^{k} \frac{-j}{i-j}}$. The verification notary group also needs to verify the main key after restoration. As long as more than two-thirds of the nodes in the notary group are honest nodes, the main key can be restored, and the transaction can continue. After the end of the transaction, the notary group will screen and identify malicious nodes. If the main key is restored correctly, digital signatures can be made. Otherwise, the transaction will be terminated, malicious nodes will be screened and removed, and the transaction will be re-initiated. After receiving the form information, the transaction notary group uses public key information to verify the digital signature and release the locked funds on both chains if the signature is correct.

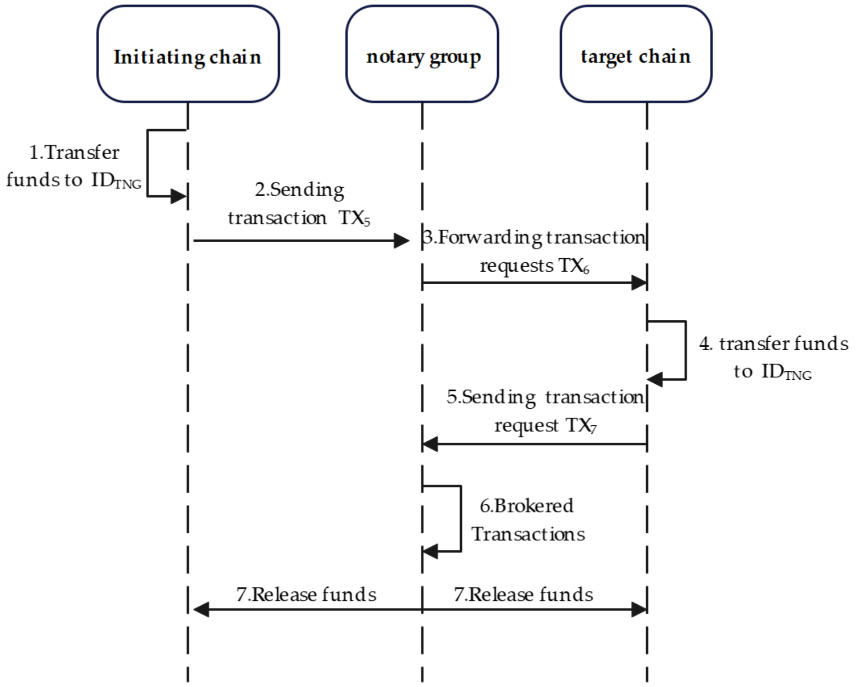
Initiating chain
notary group
target chain
1.Transfer funds to ID_{TNG}
2.Sending transaction TX5
3.Forwarding transaction requests TX6
4. transfer funds to IDTNG
5.Sending transaction request TX7
6.Brokered Transactions
7.Release funds
7.Release funds

Figure 3. Flow chart of formal transaction stage.

Algorithm 2. Formal transaction stage algorithm

```
Input: $TX$; $ID_S$; $ID_R$; $ID_{TNG}$; $ID_{TNG}$
  Output: $List$
function FORMALTRANSAction($TX$, $ID_S$, $ID_R$, $ID_{TNG}$, $ID_{TNG}$)
     S.lockList($TX_5$; $ID_S$)
     VNG.ForwordList($TX_6$, $ID_{VNG}$)
S.lockList($TX_7$; $ID_R$)
     if TX.checkContent($TX_7$ == true) then
 ReleaseTNG($ID_S$, $ID_R$, $ID_{TNG}$, $ID_{TNG}$)
     else
  SendTransaction(0)//
        break
 end if
 return $List_{TNG}$, $List_{VNG}$
 end function
```

4.2.3. Confirmation Stage

At the end of the transaction stage, to ensure that the transaction notary group has transferred the escrow funds to the account addresses of both buyers and sellers, it is necessary to verify that the notary group has confirmed the final transaction status. As shown in Figure 4 and Algorithm 3, the verification notary group in the notary group will monitor the final transaction results of the two trading parties on the two chains in real time to ensure that all the data of this transaction are successfully uploaded to the chain, and after confirming that the funds have been accurately transferred to the target account, the final transaction bill data will be generated to record the participants and execution process of this cross-chain transaction. Finally, all the data information will be safely backed up, the cross-chain transaction is now complete.

Algorithm 3. Confair transaction stage algorithm

```
Input: $TX$; $ID_S$; $ID_R$; $ID_{TNG}$; $ID_{VNG}$
Output: List
function CONFAIRTRANSAction($TX$, $ID_S$, $ID_R$, $ID_{TNG}$, $ID_{VNG}$)
VNG.MonitorList($ID_S$, $ID_R$)
  if TX.CheckContent($TX$ == TRUE) then//$TX$ is the feedback information
    VNGbbackupList()
     else
    SendTransaction(0)
    break
  end if
  return List
 end function
```

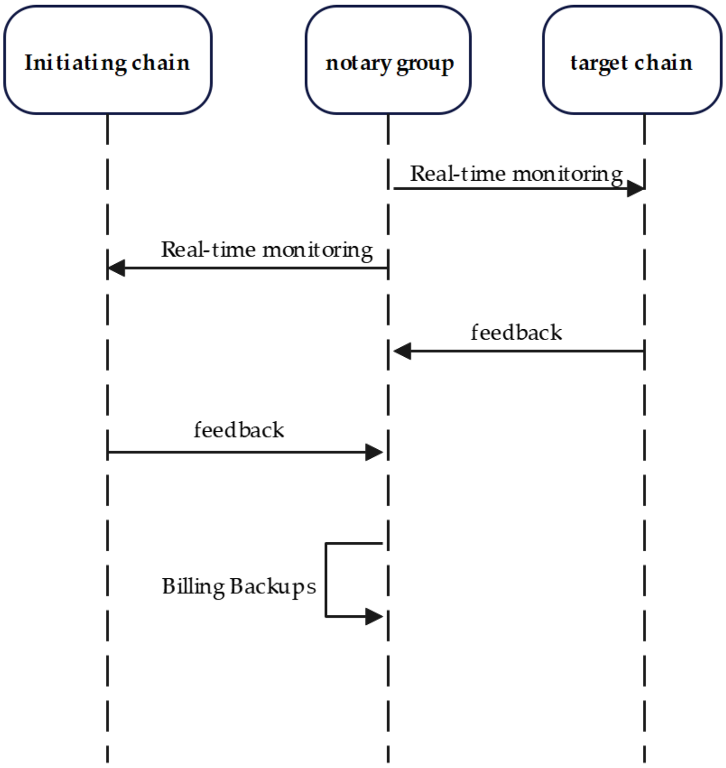

Figure 4. Flow chart of confirmation stage.

5. Performance Analysis

5.1. Security Analysis

In the process of cross-chain transactions, it will face many types of network attacks, mainly including Byzantine node attacks, brute force attacks, man-in-the-middle attacks, and privilege escalation, which cause serious damage to the system. The biggest threat comes from Byzantine node attacks, which mainly refer to the presence of malicious nodes in the network that can compromise the security of the entire system by tampering, forging, or denying messages. For example, malicious nodes may tamper with form data, causing the data received by a node to be unreliable; they may impersonate other nodes to steal key information and gain undue benefits. To address the issues mentioned above, the protocol adopts strict identity verification procedures and a decentralized threshold signature algorithm to ensure system security. First of all, a newly added notary node must provide valid proof documents and pledge a certain amount of security deposit to the notary node pool and can only become a notary after verification by other notary nodes. These measures initially ensure the legitimacy of the new node's identity. On the other hand, the protocol adopts a decentralized threshold signature algorithm that requires multiple notary nodes to complete the signature process together. Malicious behavior by attackers will be detected by the algorithm's validation model and subsequently rejected and excluded by other nodes, thus preventing significant impact on the entire system.

In a decentralized threshold signature algorithm, each participant has their own subkey s_i. During the signature process, a certain number of participants are required to recover the complete master key $s = \sum_{i=1}^{n} s_i$ before the signature can be generated. This prevents fraudulent behavior by individual or a minority of nodes. In the key verification phase, all participants randomly select a set of n dimensional vector $a_i = (a_1, a_2 \ldots a_n)$ and then calculate the product of vector a_i and the message m_i sent by other participants, denoted as v_i. Afterwards, v_i is announced to other participants to ensure that each participant's polynomial coefficients $f_i(x)$ are not leaked. Finally, all participants jointly calculate the interpolation polynomial $f_v(x)$ at point (i, v_i). By determining whether $f_v(x)$ is a $k-1$ degree polynomial, fraudulent behavior can be detected. If an attacker wants to break the encryption algorithm, it must obtain all participants' polynomial coefficients $f_i(x)$ and random vector a_i to reconstruct the original key. However, in this encryption scheme, the security of the polynomial $f_i(x)$ depends on the difficulty of solving polynomials, so we set the degree k of the polynomial very high, making it almost impossible for attackers to crack it. Additionally, the random vector a_i are randomly generated and unpredictable, so attackers cannot directly guess or try brute-force attacks on the polynomial coefficients and random vector. If an attacker attempts to impersonate a participant in a man-in-the-middle attack, during the key verification phase, it is necessary to multiply the random vector a_i with the information m_i sent by other participants, and then publish the resulting value v_i. In this way, the attacker cannot tamper with the data without knowing the vector information of the other participants. If the attacker sends incorrect data directly, other participants will generate errors in computing the shared interpolation polynomial $f_v(x)$, thereby detecting the presence of attacker interference. Therefore, in this case, a man-in-the-middle attack is ineffective.

The core defense against the malicious behavior of attackers mentioned above is to verify whether the polynomial $f(x)$ is a $k-1$ degree polynomial. The following is a discussion on its verification principle. Firstly, in the discussion of Section 3.2, we learned that $f(x) = \sum_{i=1}^{n} f_i(x)$. Then, $f_v(x)$ is an interpolation polynomial on the points (i, v_i), $i = 1, 2 \ldots n$, and $v_i = f_v(i)$. Because $v_i = \sum_{j=1}^{n} a_j m_{ji}$ and $m_{ji} = f_j(i)$, we can obtain $v_i = \sum_{j=1}^{n} a_j f_j(i)$. Let $h(x) = \sum_{i=1}^{n} a_i f_i(x)$, we can get $v_i = h(i), i = 1, 2 \ldots n$. Since the degree of $f_v(x)$ is less than or equal to $n-1$, according to $v_i = f_v(i) = h(i)$, we can conclude that $f_v(x) = h(x) = \sum_{i=1}^{n} a_i f_i(x)$. Next, we need to be proven that whenever the degrees of both $f_v(x)$ and $f(x)$ are equal to $k-1$. Assuming there exists a k degree polynomial in $f_i(x), i = 1, 2 \ldots n$, w_i represents the coefficient of x^k in $f_i(x)$. When the degree of $f_i(x)$ is $k-1$, $w_i = 0$. Since $f_i(x)$ is a $k-1$ degree polynomial if and only if $\sum_{i=1}^{n} a_i w_i = 0$. It is worth noting that since the vector $(a_1, a_2 \ldots a_n)$ is randomly generated by the participants, the probability of the equation $\sum_{i=1}^{n} a_i w_i = 0$ being satisfied is only $\frac{1}{q}$, where q is a sufficiently large prime number. Therefore, as q gets larger, this probability becomes increasingly small and can be ignored. Hence, we have proven that when $f_v(x)$ is a $k-1$ degree polynomial, the degrees of all $f_i(x), i = 1, 2 \ldots n$ are also equal to . Furthermore, since $f(x) = \sum_{i=1}^{n} f_i(x)$, it follows that the degree of $f(x)$ is also $k-1$. In conclusion, we have shown that the participants can verify the validity of the subkeys by computing $f(x)$. During the verification process, the information that participants disclose is the vector $(a_1, a_2 \ldots a_n)$ and the polynomial $f_v(x) = \sum_{i=1}^{n} a_i f_i(x)$. By using the linearity property, it can be shown that no subkey or valid key information can be obtained from $(a_1, a_2 \ldots a_n)$ and the polynomial $f_v(x) = \sum_{i=1}^{n} a_i f_i(x)$). Therefore, our scheme is unconditionally secure.

5.2. Experimental Analysis

The simulation experiment environment of this scheme is hosted on a machine with an Intel(R) Core (TM) i7-5500U CPU @ 2.40 GHz processor, 8 GB RAM running Windows 10. The blockchain is built on an Ubuntu on Windows virtual machine with the same configuration as the host machine. The built blockchain is a Fisco Bcos alliance chain with a single group of fifty nodes, version 2.8.0, and both blockchains are configured similarly.

5.2.1. Improved Notary Ranking Algorithm Election Effect

This experiment was conducted on a blockchain, and 50 nodes on the chain were selected to form a notary group to validate the effectiveness of the original PageRank algorithm and the improved algorithm. The experiment begins, by initializing the trust relationships of each node and assigning a number to each node, forming a node relationship graph. Among them, nodes numbered from 1 to 10 have more trust relationships, while the remaining 40 nodes have fewer trust relationships. It is worth noting that the last three nodes, numbered 48, 49, and 50, do not have any trust relationships, indicating that they are new nodes added to the notary group. Then, each node is initialized and assigned, at this time the credit value of each node is **1/50**. Afterward, iterations are performed, during which new trust relationships are randomly established based on the credit value of each node (nodes with higher reputation scores have a higher probability of being selected and will, therefore, establish more trust relationships). Eventually, each node will have a relatively stable credit value.

The experimental results are shown in Figure 5. In the verification of the original PageRank algorithm, nodes numbered 1 to 10 have more trust relationships, and their credit values increase slightly with each iteration, while the other 40 nodes have a decreasing credit value for each iteration due to the lack of trust relationships. Therefore, after multiple iterations, the credit value of all nodes tends to stabilize, with the top 10 nodes having a much higher value than the others, resulting in a significant difference between them. It is worth noting that the last three newly added nodes, due to the lack of trust relationships, have a very little chance of being selected regardless of their effectiveness, and cannot establish trust relationships with other nodes, resulting in their credit values remaining very low. It can be seen from this that the original PageRank algorithm is not very friendly to newly added nodes, and it is difficult for their credit values to increase. On the contrary, if a node joins the group of notaries early on and establishes more trust relationships, its final credit value will be high, and it will have a greater chance of being selected to participate in transactions. This also means that the entire transaction power will be concentrated on older nodes, increasing the risk of centralization.

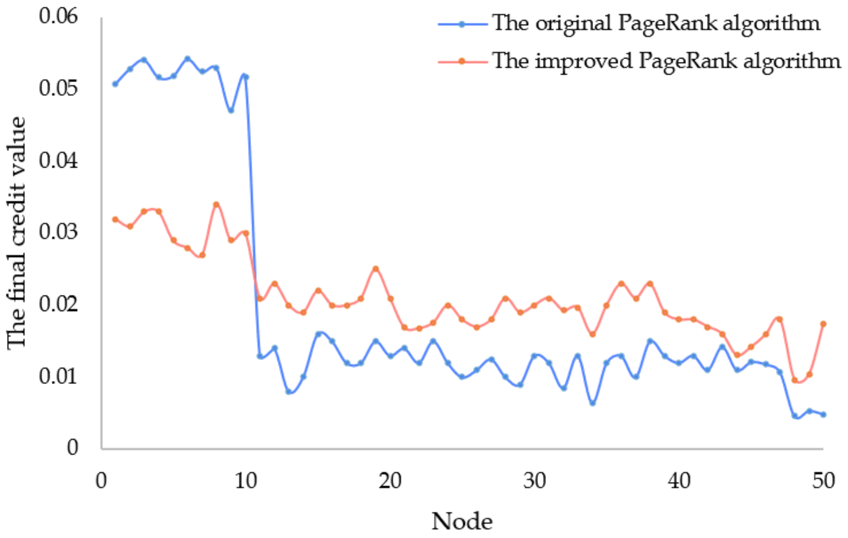

Figure 5. Sorting results of the original PageRank algorithm and the improved algorithm.

Later on, the improved PageRank algorithm was further validated in experiments. For this algorithm, additional parameters were added such as average response time, deposit ratio, and historical completed transaction volume to enhance the evaluation system for credit value. After multiple iterations, the credit value for each node tends to stabilize. The improved algorithm shows a more stable characteristic compared to the original algorithm, resulting in a significant reduction in the gap between the final credit value of the first 10 nodes and the other 40 common nodes. The overall credit value of the first 10 nodes has reduced by around 40%, while the overall credit value of other common nodes has increased by around 90%. It is noteworthy that after multiple iterations, the credit value of newly added nodes in the improved algorithm has increased by more than double. Particularly, the final credit value of the last node has significantly increased, reaching the average level of the old nodes, especially when its three parameter values are assigned high values. It can be concluded that after the algorithm improvement, the credit value evaluation of each node pair is more comprehensive and complete, and the problem of a few nodes having excessively high credit values will not occur. At the same time, the improved algorithm is friendly to new nodes, and the credit value of newly added nodes will gradually increase, thus increasing the chances of being selected to participate in transactions gradually. This effectively avoids the concentration of transaction rights in a few old nodes, reduces centralization risks, and makes the entire cross-chain trading system more secure and reliable.

5.2.2. Transaction Time and Transaction Success Rate

In this experiment, a total of 100 cross-chain transaction requests are initiated. As shown in Table 3, when all nodes in the notary group are honest, the average time for cross-chain transactions using this protocol is about 7.4 s. The first phase takes a shorter time because all operations are performed off-chain, with an average time of 0.66 s. The second stage requires a transaction to be completed on both chains, and the total time from initiating the transaction to the notary group releasing the funds is 4.65 s. The third stage takes 2.08 s from the release of funds by the notary group to the confirmation of the completion of the transaction by the verification notary group. In the case of traditional single-node notaries, the average time consumed by a cross-chain transaction is 7.1 s, and the average difference in transaction time between the two is about 0.3 s. Therefore, it can be concluded that the impact of the protocol on transaction time can be neglected.

Table 3. Average time spent in each stage.

Stage Name	Time Consumption
Pre-transaction stage	0.658219
Transaction Stage	4.652597
Confirmation stage	2.082395
Total	7.393211

Meanwhile, this experiment also tested the overall efficiency of the system when there are malicious nodes in the network. The experiment calculated the cross-chain transaction time under different percentages of malicious notaries in the notary group, namely 5%, 10%, 20%, 30%, and 40%. The experimental results are shown in Figures 6 and 7, in the case of a single-node notary mode, as the number of malicious nodes increases, the overall efficiency of cross-chain transactions is gradually decreasing. This is mainly because the election of malicious nodes can cause the transaction to fail, and failed transactions will be re-initiated in the system. Therefore, as the percentage of malicious notaries in the notary group increases, the success rate of transactions will gradually decrease, and the average transaction time will gradually increase. In the three-stage cross-chain protocol, as long as the number of malicious nodes in the elected notary group does not exceed one-third, it will not have a significant impact on the overall transaction time and success rate. This is mainly because during the transaction process, the protocol separates transaction and verification, and both transaction and verification are carried out through the transaction notary group and the verification notary group. Even if multiple nodes act maliciously, the main key can still be successfully restored during the decentralized threshold signature verification process, ensuring the effective guarantee of transaction success rate. However, If the number of malicious nodes in the transaction notary group exceeds one-third, the advantage of the protocol will be lost. This will cause a decrease in the success rate and an increase in the average transaction time. In summary, the overall performance of the three-stage cross-chain protocol is higher than that of the traditional single-node notary model, and it has a stronger ability to resist malicious attacks.

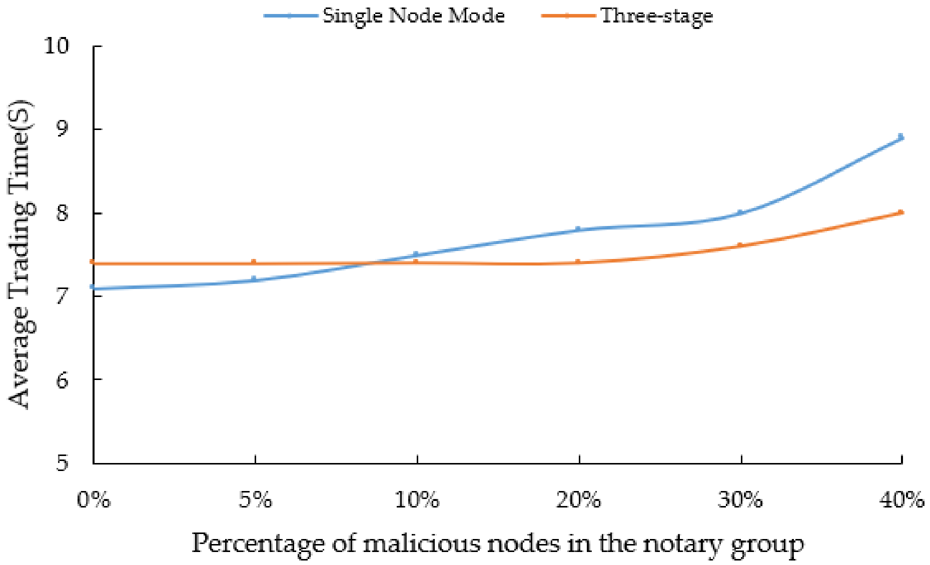

Figure 6. Average time to trade.

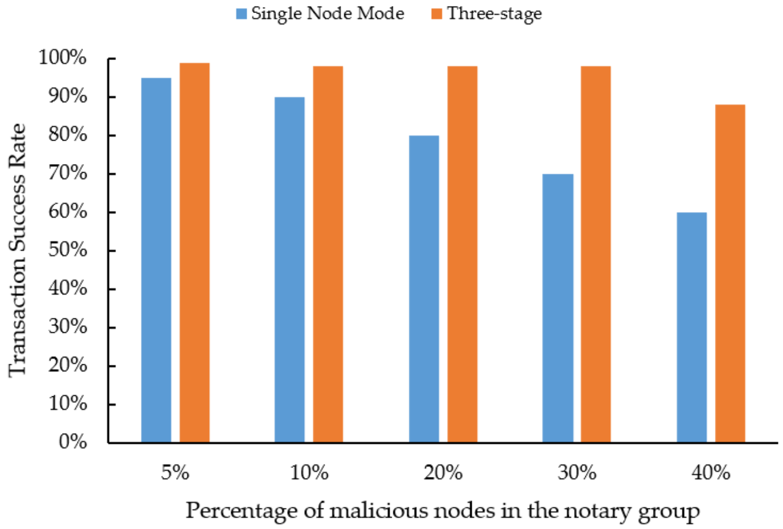

Figure 7. Transaction success rate.

5.2.3. Comparative Analysis

In this article, the evaluation indicators for cross-chain protocols mainly include reliability, privacy, scalability, and regulatory ability, among others. Reliability refers to the stability of the system before and after the transaction is executed. It represents whether the protocol can detect malicious behavior during the transaction process and ensure the safety of users' funds in the event of an attack; Privacy refers to whether the mechanism for hiding cross-chain transaction information and identity is well-developed; Scalability refers to the number of blockchain systems that the transaction network can support and whether it supports transactions between heterogeneous chains; Regulatory ability refers to whether the protocol has a regulatory model and supports identity authentication. This section will compare and analyze the three-stage cross-chain protocol and other cross-chain protocols based on the notary mechanism from seven aspects: reliability, privacy, scalability, regulatory ability, cross-chain type (HO represents homogeneous chain and HE represents heterogeneous chain), and the advantages and disadvantages of the protocol. The specific analysis results are shown in Tables 4 and 5.

Table 4. Comparative analysis results of the protocol.

Protocol Name	Reliability	Privacy	Scalability	Regulatory Ability	Type
PCRM [30]	high	low	medium	low	HO, HE
CCCES [31]	high	low	high	low	HO, HE
DeXTT [32]	medium	low	medium	low	HO
XCLAIM [33]	high	low	high	low	HO
Three-stage	high	medium	medium	medium	HO

Table 5. Comparative analysis results of protocol advantages and disadvantages.

Protocol Name	Advantages	Disadvantages
PCRM [30]	Fast verification of cross-chain access to information	High latency in unstable network conditions.
CCCES [31]	High portability and high usability	Low privacy
DeXTT [32]	Low transaction costs	Limited application scenarios
XCLAIM [33]	Meet the atomicity of the transaction	On-chain tokens only meet specific smart contract requirements
Three-stage	Multi trusted nodes and High security	High requirements on computing resources

From Tables 4 and 5, it can be concluded that in the aspect of reliability, the decentralized threshold signature algorithm can timely detect malicious attacks and thereby the malicious nodes will be rejected and excluded by other nodes, which will not cause significant damage to the entire system. Therefore, the three-stage cross-chain protocol has high reliability; In the aspect of privacy, the three-stage cross-chain protocol eliminates the reliance on a single trusted node but is not fully decentralized, thus the privacy level is medium; In the aspect of scalability, the three-stage cross-chain protocol divides transactions into three stages that are executed in order. The notary nodes in the new blockchain can conduct cross-chain transactions as long as they have accounts on other chains. On the other hand, this protocol currently does not support transactions on heterogeneous chains, so the scalability level is medium.

In the aspect of the regulatory ability, the verification model of the three-stage cross-chain protocol is the verification notary group. On the other hand, the protocol is responsible for data security and reliability through the decentralized threshold signature algorithm. When a malicious node attempts to impersonate a notary node for participation in transactions, the decentralized threshold signature algorithm can determine that the malicious node is a forgery by computing polynomial counts during the key verification stage, thus achieving some degree of identity authentication. Therefore, the level of regulatory ability is medium. In the aspect of cross-chain type, the experimental results of the three-stage cross-chain protocol demonstrate its support for cross-chain transactions on homogeneous chains. The advantage of the three-stage cross-chain protocol is that it eliminates the trust in a single trusted node, avoiding centralization issues. The disadvantage is that the decentralized threshold signature algorithm requires more computing resources when verifying the main key information. In summary, the overall metrics of the three-stage cross-chain protocol based on the notary node group are higher than those of other protocols.

6. Conclusions

This article proposes a three-stage cross-chain protocol based on a notary group, which effectively solves the problem of relying on single-trust nodes in the notary mechanism and achieves more efficient and cost-effective cross-chain interaction. In the protocol, an improved PageRank sorting algorithm is used to elect the notary group, and each node's performance is evaluated from multiple dimensions. Compared with the original PageRank algorithm, the new algorithm reduces the credit value of central nodes by about 40% and increases the final credit value of ordinary nodes by about 90%, avoiding centralized transactions and reducing centralization risks. The notary nodes elected by the protocol will be divided into transaction notary groups and validation notary groups. Transaction notary groups are responsible for the accurate execution of transaction processes, while validation notary groups are responsible for the security and reliability of transactions. Both groups are validated using decentralized threshold digital signature algorithms, which can resist malicious attacks by one or a small number of nodes, showing the advantages of fast transaction speed and high security. At the same time, the protocol divides cross-chain transactions into three stages, and each stage progresses according to the protocol requirements to ensure trusted cross-chain interaction and achieve cross-chain transaction synchronization. Experimental results show that as long as the number of malicious nodes in the notary group does not exceed one-third, the three-stage cross-chain protocol can effectively ensure the security of cross-chain transactions, and the success rate of transactions remains above 95%, basically solving the centralization problem. In the next phase, we will further optimize the protocol model from the perspective of storage efficiency and reduce computational consumption during transaction verification.

Author Contributions: Conceptualization, X.S. and L.C.; methodology, Z.Y. and Q.Z.; software, L.C.; validation, L.C. and Z.Y.; formal analysis, Z.Y. and Q.Z.; investigation, L.C. and Q.Z.; resources, X.S.; data curation, X.S. and Q.Z.; writing—original draft preparation, L.C.; writing—review and editing, Z.Y. and Q.Z.; supervision, Z.Y.; project administration, X.S.; funding acquisition, X.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Major Public Welfare Project of Henan Province, grant number 201300210300; Key Science and Technology Project of Henan Province, grant number 222102210168; Open Fund of Henan Key Laboratory of Network Cryptography Technology, grant number LNCT2022- A12.

Data Availability Statement: The source code in this study is available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Blockchain Technology Market Size, Share and COVID-19. Available online: https://www.fortunebusinessinsights.com/industry-reports/blockchain-market-100072 (accessed on 24 May 2023).
2. Lee, Y.; Son, B.; Jang, H.; Byun, J.; Yoon, T.; Lee, J. Atomic cross-chain settlement model for central banks digital currency. *Inf. Sci.* **2021**, *580*, 838–856. [CrossRef]
3. Ye, J.; Pang, C.J.; Li, X.H.; Zhang, X.; Liu, L. Blockchain-based supply chain data hierarchical access control mechanism. *China J. Univ. Electron.* **2022**, *51*, 408–415.
4. Yuan, H.N.; Wang, R.J.; Zheng, B.W.; Wu, B.Y. Design and implementation of cross-chain trusted EMR sharing system based on fabric. *China J. Comput. Sci.* **2022**, *49*, 490–495, 638.
5. Cha, S.C.; Meng, W.Z.; Li, W.W.; Yeh, K.H. A blockchain-enabled IoT auditing management system complying with ISO/IEC 15408-2. *Comput. Ind. Eng.* **2023**, *178*, 109091. [CrossRef]
6. Zhang, X.Y.; Chen, J.W.; Zhou, Y.; Jiang, S.R. Privacy-preserving cross-chain payment scheme for blockchain-enabled energy trading. In Proceedings of the 2021 IEEE/CIC International Conference on Communications in China (ICCC), Xiamen, China, 28–30 July 2021; pp. 154–196.

7. Rafael, B.; Andre, V.; Sregio, G.; Miguel, C. A survey on blockchain interoperability: Past, present, and future trends. *ACM Comput. Surv.* **2022**, *54*, 168.
8. Zabka, P.; Foerster, K.; Schmid, S.; Decker, C. Empirical evaluation of nodes and channels of the lightning network. *Pervasive Mob. Comput.* **2022**, *83*, 101584. [CrossRef]
9. Yin, L.Y.; Xu, J.; Tang, Q. Sidechains with fast cross-chain transfers. *IEEE Trans. Dependable Secur. Comput.* **2022**, *19*, 3925–3940. [CrossRef]
10. Westerkamp, M.; Eberhardt, J. zkRelay: Facilitating sidechains using zkSNARK-based chain-relays. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 7–11 September 2020; pp. 378–386.
11. Xiong, A.P.; Liu, G.H.; Zhu, Q.Y.; Jing, A.K.; Loke, S. A notary group-based cross-chain mechanism. *Digit. Commun. Netw.* **2022**, *8*, 1059–1067. [CrossRef]
12. AtomicDEX and Atomic Swaps. Available online: https://github.com/KomodoPlatform/atomicDEX-API (accessed on 24 May 2023).
13. Cosmos: A Network of Distributed Ledgers. Available online: https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md (accessed on 24 May 2023).
14. Polkadot: Vision for a Heterogeneous Multi-Chain Framework. Available online: https://polkadot.network/PolkaDotPaper.pdf (accessed on 24 May 2023).
15. Ye, S.J.; Wang, X.Y.; Xu, C.C.; Sun, J.L. BitXHub: Side-relay chain based heterogeneous blockchain interoperable platform. *Comput. Sci.* **2020**, *47*, 294–302.
16. Liao, M.H.; Li, R.H.; Dai, Q.Q.; Wang, G.R. Efficient personalized PageRank computation: A spanning forests sampling based approach. In Proceedings of the 2022 International Conference on Management of Data, Philadelphia, PA, USA, 12–17 June 2022; pp. 2048–2061.
17. Liu, Y.X.; Harn, L.; Yang, C.; Zhang, Y.Q. Efficient (n, t, n) secret sharing schemes. *J. Syst. Softw.* **2012**, *85*, 1325–1332. [CrossRef]
18. Manevich, Y.; Akavia, A. Cross chain atomic swaps in the absence of time via attribute verifiable timed commitments. In Proceedings of the 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P), Genoa, Italy, 6–10 June 2022; pp. 606–625.
19. Shadab, N.; Houshm, F.; Lesani, M. Cross-chain transactions. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2–6 May 2020; pp. 1–9.
20. Nadahalli, T.; Khabbazian, M.; Wattenhofer, R. Grief free atomic swaps. In Proceedings of the 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China, 2–5 May 2022; pp. 1–9.
21. Deshpande, A.; Herlihy, M. Privacy-preserving cross-chain atomic swaps. In Proceedings of the International Conference on Financial Cryptography and Data Security, Cham, Switzerland, 7 August 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 540–549.
22. Liu, F.; Zhang, J.H.; Zhou, J.J.; Li, M.; Kong, D.L.; Yang, J.; Qi, J.Y.; Zhou, A.M. Novel hash-time-lock-contract based cross-chain token swap mechanism of blockchain. *China J. Comput. Sci.* **2022**, *49*, 336–344.
23. Sigwart, M.; Frauenthaler, P.; Spanring, C.; Sober, M.; Schulte, S. Decentralized cross-blockchain asset transfers. In Proceedings of the 2021 Third International Conference on Blockchain Computing and Applications (BCCA), Tartu, Estonia, 15–17 November 2021; pp. 34–41.
24. Pillai, B.; Biswas, K.; Hóu, Z.; Muthukkumarasamy, V. The Burn-to-Claim cross-blockchain asset transfer protocol. In Proceedings of the 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS), Singapore, 28–31 October 2020; pp. 119–124.
25. Li, Y.X.; Weng, J.; Li, M.; Wu, W.; Weng, J.S.; Liu, J.N.; Hu, S. ZeroCross: A sidechain-based privacy-preserving cross-chain solution for monero. *J. Parallel Distrib. Comput.* **2022**, *169*, 301–316. [CrossRef]
26. Xu, Z.; Liu, C.F.; Wang, S.T.; Zhang, P. An AST-based consistency maintenance scheme for cross-chain digital assets. *CCF Trans. Pervasive Comput. Interact.* **2022**, *4*, 142–157. [CrossRef]
27. Zhang, S.B.; Xie, T.X.; Gai, K.K.; Xu, L. ARC: An asynchronous consensus and relay chain-based cross-chain solution to consortium blockchain. In Proceedings of the 2022 IEEE 9th International Conference on Cyber Security and Cloud Computing (CSCloud)/2022 IEEE 8th Inter-national Conference on Edge Computing and Scalable Cloud (EdgeCom), Xi'an, China, 25–27 June 2022; pp. 86–92.
28. Tian, H.Y.; Xue, K.P.; Luo, X.Y.; Li, S.H.; Xu, J.; Liu, J.Q.; Zhao, J.; Wei, D. Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3928–3941. [CrossRef]
29. Wu, X.Z. Cross-chain workflow model based on trusted relay. In Proceedings of the ACM Turing Award Celebration Conference (ACM TURC 2021), Hefei, China, 30 July–1 August 2021; pp. 49–53.
30. Wu, Z.H.; Xiao, Y.; Zhou, E.Y.; Pei, Q.Q.; Wang, Q. A solution to data accessibility across heterogeneous blockchains. In Proceedings of the 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS), Hong Kong, China, 2–4 December 2020; pp. 414–421.
31. Hei, Y.M.; Li, D.W.; Zhang, C.; Liu, J.W.; Liu, Y.Z.; Wu, Q.H. Practical AgentChain: A compatible cross-chain exchange system. *Future Gener. Comput. Syst.* **2022**, *130*, 207–218. [CrossRef]

32. Borkowski, M.; Sigwart, M.; Frauenthaler, P.; Hukkinen, T.; Schulte, S. Dextt: Deter-ministic cross-blockchain token transfers. *IEEE Access* **2019**, *7*, 111030–111042. [CrossRef]
33. Zamyatin, A.; Harz, D.; Lind, J.; Panayiotou, P.; Gervais, A.; Knottenbelt, W. XCLAIM: Trustless, interoperable, cryptocurrency-backed assets. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 193–210.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.