A Cross-Chain Mechanism Based on Hierarchically Managed Notary Group

Hongliang Tian, Zhiyang Ruan, Zhong Fan
School of Electrical Engineering, Northeast Electric Power University, Jilin 132012, China

***Abstract*—Blockchain technology, characterized by decentralization, immutability, traceability, and transparency, provides innovative solutions for data management. However, the limited cross-chain interoperability between blockchains hampers their broader application and development. To address this challenge, this paper proposes a Cross-Chain Mechanism Based on Hierarchically Managed Notary Group, abbreviated as HMNG-CCM, which enables secure and efficient cross-chain transactions between blockchains. To mitigate the centralization issue inherent in traditional cross-chain mechanism based on notary, an innovative notary group management approach is introduced. This approach implements hierarchical management by categorizing notaries into three levels—junior notary, intermediate notary, and senior notary—thereby effectively mitigating the centralization problem. Additionally, a functional division mechanism for notary is designed, wherein the roles of transaction processing and verification within the cross-chain transaction process are separated to enhance system reliability. Furthermore, to tackle the complexity of notary reputation evaluation, a reputation assessment scheme based on an improved PageRank algorithm is proposed. Differentiated reputation evaluation strategies are developed for junior and intermediate notaries to ensure fairness and rationality in the assessment process. The effectiveness of this scheme is validated through experiments conducted on the Hyperledger Fabric platform. The experimental results demonstrate that the proposed mechanism exhibits strong robustness against malicious notaries while significantly improving transaction speed and success rate. This study offers new theoretical and practical foundations for the optimization and advancement of blockchain cross-chain technology.**

Keywords*—Blockchain; cross-chain; notary group; hierarchical management; reputation evaluation

I. Introduction

Blockchain technology integrates multiple techniques, including hash algorithms, digital signatures, and consensus mechanisms, exhibiting characteristics such as decentralization, immutability, traceability, and transparency [1]. Since Satoshi Nakamoto proposed Bitcoin [2], the significance of blockchain technology has extended beyond the realm of cryptographic digital currencies. Ethereum [3], through the implementation of smart contracts, has extended blockchain technology to domains such as financial services [4], healthcare systems [5], and the Internet of Things [6], offering innovative solutions for data management. However, as application scenarios continue to expand, the isolation among blockchain systems has become increasingly prominent [7]. This isolation constrains the performance and security of blockchains and impedes their application in complex business scenarios. Currently, the blockchain ecosystem exhibits characteristics of diversity and fragmentation, with most blockchain systems remaining independent information silos [8]. For instance, systems such as Bitcoin, Ethereum, and Hyperledger Fabric [9], due to their adoption of distinct protocol standards, consensus mechanisms, and technical architectures. This independence hinders cross-chain data exchange and value transfer [10]. These barriers have been overcome by the emergence of cross-chain technology [11], which facilitates the cross-chain interaction of data and assets. This technology establishes an interconnected blockchain network ecosystem and lays the foundation for the further development of blockchain technology.

Existing cross-chain technologies encompass Notary Schemes [12], Relays [13], Hash-locking [14], and Distributed Private Key Control [15]. Among these, the Notary Schemes simplifies transactions processes between blockchains by introducing third-party notary nodes, offering advantages such as ease of implementation and high flexibility, which have led to its widespread adoption across various cross-chain scenarios. However, this mechanism's excessive reliance on a single notary node introduces the risk of single point of failure and significantly increases the system's centralization, thereby undermining the security and reliability of blockchain systems. Consequently, existing notary mechanisms commonly face challenges, including high centralization, insufficient generality in reputation evaluation schemes, and low efficiency in cross-chain transactions. To address these challenges, this paper proposes a Cross-Chain Mechanism Based on Hierarchically Managed Notary Group (HMNG-CCM), aimed at achieving secure and efficient cross-chain transactions between blockchains.

The contributions of this paper are as follows:

1) This paper proposes an innovative notary management scheme. The scheme implements hierarchical management by dividing the notary group into three categories: junior notaries, intermediate notaries, and senior notaries. This mechanism reduces the degree of system centralization, effectively distributing the trust risks associated with notaries in cross-chain transactions.

2) This paper designs a notary functional division mechanism. This mechanism explicitly separates the functions of transaction execution and verification within the cross-chain transaction process, assigning specific task responsibilities to different levels of notaries. Specifically, junior and intermediate notaries are tasked with transaction execution,

while senior notaries focus on transaction verification. This functional division mechanism not only optimizes the transaction process but also enhances the robust-ness of the cross-chain system.

3) This paper proposes a reputation assessment scheme based on an improved PageRank algorithm for ranking notaries. Addressing the distinct roles undertaken by notaries of varying levels in cross-chain transactions, differentiated reputation evaluation strategies are developed for junior and intermediate notaries to ensure fairness and rationality in the reputation assessment process. Through this algorithm, the system can dynamically adjust the reputation rankings of notaries, effectively enhancing the trustworthiness and security of the cross-chain transaction system.

The remainder of this paper is structured as follows. Section II discusses recently proposed cross-chain interoperability schemes. Section III provides a detailed description of the scheme proposed in this paper. Section IV compares the performance of the scheme proposed in this paper with that of other schemes and provides its security analysis. Finally, Section V concludes this paper.

II. Related Works

In recent years, based on the four commonly recognized cross-chain technologies, various cross-chain transaction schemes [16], have been successively proposed. Enhancing cross-chain technology requires addressing multiple challenges, including system reliability [17], scalability [18], performance [19], and security [20].

Hou et al. [21] and Wang et al. [22], employed relay chains as communication bridges to enable cross-chain transactions, reducing the integration costs of heterogeneous blockchains and improving the performance of cross-chain systems; however, the protection of cross-chain data still offers room for optimization. Wu et al. [23], introduced an encryption scheme based on smart contracts, establishing constrained relationships between relay chains and other blockchains to enhance system security and privacy protection. Furthermore, Wang et al. [24], enhanced the scalability of relay chain-based cross-chain systems through sharding operations applied to the relay chain. Nevertheless, the application of existing relay chain technologies in cross-chain transactions continues to face challenges, including implementation complexities, suboptimal performance, and inadequate system stability [25].

Li et al. [26], integrated Hash Time-Locked Contract (HTLC) with a virtual account verification mechanism, thereby improving the success rate of cross-chain transactions. Wang et al. [27], incorporated a dynamic premium adjustment mechanism and a credit mechanism into HTLC, proposing a Hash Time Lock with Dynamic Premium Based on Credit in Cross-Chain Transaction to address issues of transaction default and reduced efficiency in cross-chain transactions. Yu et al. [28], applied an optimized HTLC to a Multi-Agent System, enhancing security and transparency. However, when handling complex, high-value transactions, HTLC continues to exhibit significant limitations in scalability and transaction efficiency [29].

Yu et al. [30], proposed a key management scheme based on distributed identity, mitigating the pervasive issue of trust centralization in cross-chain transactions. Zhao et al. [31], further leveraged distributed private key technology to eliminate reliance on trusted nodes, thereby safeguarding the interests of participants in secret-sharing protocols and avoiding the risk of single-point failures. Ren et al. [32], integrated distributed keys with a Proof of Trust Contribution consensus algorithm and a non-interactive zero-knowledge proof protocol, enhancing both the efficiency of key generation and the security of key management. However, as the number of nodes increases, distributed private key control technology faces the challenge of balancing computational efficiency with system security.

Compared to the other three cross-chain schemes, the notary mechanism offers advantages such as low implementation cost, rapid transaction processing speed, and support for cross-chain transactions across multiple blockchains, proving particularly efficient in trusted environments. The Interledger Protocol [33], proposed by Ripple Labs, focuses on enabling cross-chain payments through a universal framework and serves as a quintessential example of the notary mechanism. However, its conflict with the core decentralized ethos of blockchain technology raises significant security concerns. Xiong et al. [34], introduced a notary committee comprising multiple notaries, selecting notaries based on reputation to handle cross-chain transactions, thereby eliminating dependence on a single notary and enhancing the system's resilience against malicious notaries. Nevertheless, the comprehensiveness of notary reputation assessment remains inadequate. To address this issue, Chen et al. [35], proposed a dynamic reputation management scheme based on the past transaction behavior of nodes. This scheme designs reputation evaluation metrics by analyzing prevalent security threats and incorporates a Particle Swarm Optimization algorithm to dynamically adjust metric weights, enabling adaptation to varying frequencies of malicious behavior. However, as it considers only common blockchain security threats, the scheme exhibits limitations in specific cross-chain scenarios.

Addressing the strengths and weaknesses of existing cross-chain schemes, this paper proposes the HMNG-CCM. This mechanism categorizes the notary group into three levels—junior notaries, intermediate notaries, and senior notaries—based on reputation, aiming to optimize the notary election process and reduce the system's centralization. Concurrently, it designates that only intermediate and junior notaries are responsible for transaction execution, while senior notaries are exclusively tasked with transaction verification, further refining the cross-chain transaction process. Additionally, differentiated reputation evaluation strategies are established for junior and intermediate notaries, and an improved PageRank algorithm is introduced to dynamically adjust the reputation of notary nodes, ensuring the fairness and rationality of the assessment.

III. Proposed Scheme

In this section, the architecture and operational principles of the HMNG-CCM are elaborated in detail. Through a

comprehensive cross-chain protocol (preparation phase, transaction phase, and confirmation phase), this study designs and implements a cross-chain model based on notary group, an improved PageRank algorithm, a hierarchical management scheme of the notary group, and a hierarchical notary election process.

A. Cross-Chain Model Based on Notary Group

The cross-chain model based on a hierarchically managed notary group proposed in this paper ensures the security of cross-chain interoperability by introducing a notary group and subjecting it to hierarchical management. As illustrated in Fig. 1, the system comprises three key components: the notary group, the source chain, and the target chain.

1) Notary group: This component consists of multiple nodes, each possessing at least one account on both the source chain and the target chain. During the initialization of the notary group, the system leverages smart contracts to create two margin pool accounts—one on the source chain and one on the target chain—and generates a set of notary nodes. The reputation of each node is calculated using an improved PageRank algorithm, and based on these reputation rankings, nodes are classified into junior notaries, intermediate notaries, and senior notaries, thereby establishing and maintaining the management framework of the notary group.

2) Source chain: This component refers to the blockchain where the sender of a cross-chain transaction resides. During the cross-chain transaction process, the primary participants on the source chain include the sender node, notary nodes, and the margin pool account maintained by the notary group on the source chain.

3) Target chain: This component refers to the blockchain where the receiver of a cross-chain transaction resides. During the cross-chain transaction process, the primary participants on the target chain include the receiver node, notary nodes, and the margin pool account maintained by the notary group on the target chain.

B. Reputation Evaluation Scheme Based on an Improved PageRank Algorithm

The PageRank algorithm is a link analysis-based webpage ranking method designed to evaluate the relative importance of webpages within a hyperlinked network. Its fundamental expression is given as follows:

$$PR(A) = \frac{1-d}{N} + d \cdot \sum_{i \in M(A)} \frac{PR(j)}{L(j)} \quad (1)$$

In Eq. (1), $PR(A)$ represents the PageRank value of webpage A, $M(A)$ represents the set of webpages linking to webpage A, $L(j)$ indicates the number of outbound links from webpage j, N signifies the total number of webpages, and d is the damping factor, which models the random navigation behavior of users between webpages. This algorithm iteratively computes values until convergence, yielding the importance ranking of each webpage.

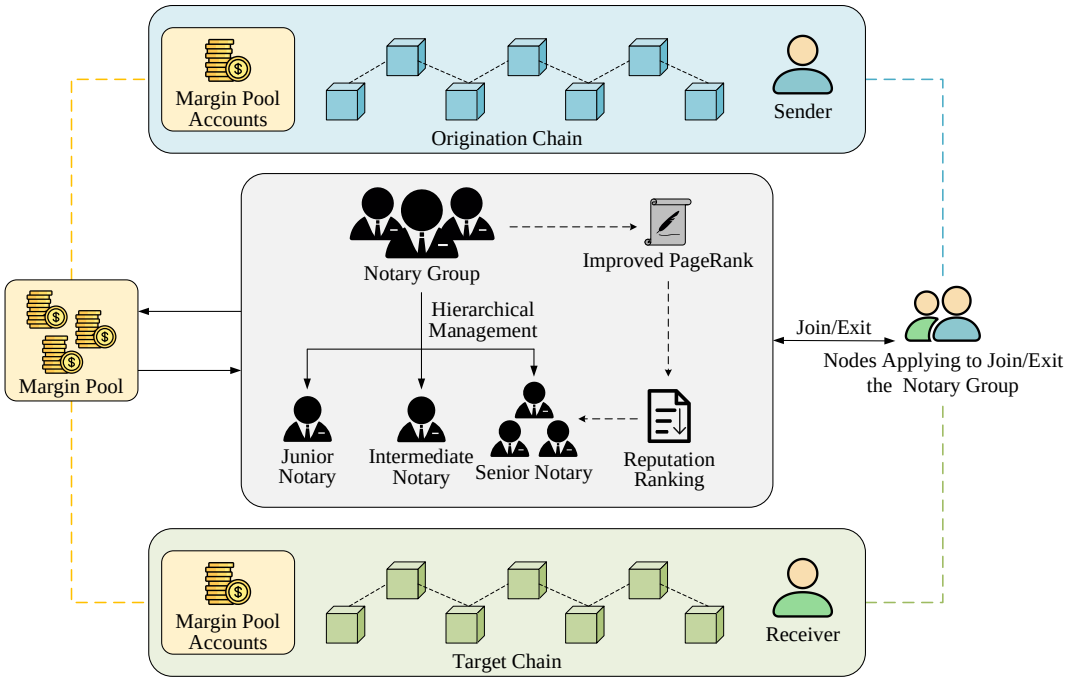


Fig. 1. Cross-chain model based on notary group.

Intermediate notaries primarily assess the comprehensive reputation of their nodes by incorporating the historical transaction success rate, transaction processing efficiency, and margin of the nodes. Table I presents the attributes of each parameter for intermediate notaries.

TABLE I. LIST OF INTERMEDIATE NOTARY PARAMETER ATTRIBUTES

Reputation Metrics	Parameter Name	Weight
Trust Relationships	*PR(j)/L(j)*	0.5
Historical Transaction Success Rate	*HTSR*	0.2
Transaction Processing Efficiency	*TPE*	0.2
Margin	*M*	0.1

Two assumptions are presented here:

1) Quantity assumption: It is assumed that a notary node exists, and if a substantial number of other notary nodes establish trust relationships with it, this indicates that the notary node possesses a high reputation.

2) Quality assumption: It is assumed that a notary node exists, and if another notary node with a high reputation establishes a trust relationship with it, the former notary node will be conferred a correspondingly high reputation.

$PR(j)/L(j)$ reflects the degree of trust that other nodes place in the given notary node. If a trust relationship exists between two nodes, they can mutually transfer reputation. Based on Quantity Assumption and Quality Assumption, it follows that the more trust relationships a notary node possesses, the greater the reputation transferred to it, resulting in a higher reputation for that node. $PR(j)/L(j)$ is a critical factor in the proposed reputation assessment scheme and is therefore assigned a weight of 0.5 as a foundational parameter.

$HTSR$ is utilized to measure the proportion of transactions successfully completed by a notary node among those in which it participates, thereby reflecting the node's transaction success rate. Consequently, $HTSR$ is assigned a weight of 0.2.

$$HTSR = \frac{Success - Fail}{Success + Fail + \varphi} \tag{2}$$

In Eq. (2), *Success* represents the number of successful transactions among those in which the notary node participates, $Fail$ denotes the number of failed transactions, and φ is a very small constant.

TPE is primarily employed to evaluate the transaction processing capability of a notary node. A shorter transaction time indicates greater efficiency of the node in processing transactions. Its weight is set at 0.2.

$$TPE = \frac{1}{n}\sum_{k=1}^{n}\frac{1}{t_k} \tag{3}$$

In Eq. (3), t_k represents the time cost for the notary node to successfully complete the k-th transaction, while n denotes the total number of transactions that the notary node has successfully completed.

The margin parameter M reflects the amount of the deposit paid by a notary node upon joining the notary group. A higher margin corresponds to greater losses for the node in the event of malicious behavior. The weight of M is set at 0.1.

$$M(i) = \frac{M_i - M_{\min}}{M_{\max} - M_{\min}} \tag{4}$$

In Eq. (4), $M_{\max}$ represents the maximum margin amount among all current nodes, $M_{\min}$ denotes the minimum margin amount, and $M(i)$ signifies the normalized result of the margin amount paid by node i.

The improved PageRank algorithm is presented in Eq. (5):

$$PR(i) = \frac{1-d}{N} + d \cdot [0.5 \sum_{j \in M(i)} \frac{PR(j)}{L(j)} + 0.2HTSR(i) + 0.2TPE(i) + 0.1M(i)] \tag{5}$$

In Eq. (5), $PR(i)$ represents the reputation of node i, N denotes the total number of notary nodes, and d is the damping factor, set at 0.85. $PR(j)$ indicates the reputation of node j, while $L(j)$ signifies the number of nodes evaluated by node j.

The reputation evaluation strategy for junior notaries incorporates not only the node's historical transaction success rate, transaction processing efficiency, and margin, but also the time a node waits to become a transaction notary. Table II lists the attributes of each parameter for junior notaries.

TABLE II. LIST OF JUNIOR NOTARY PARAMETER ATTRIBUTES

Reputation Metrics	Parameter Name	Weight
Trust Relationships	*PR(j)/L(j)*	0.4
Historical Transaction Success Rate	*HTSR*	0.2
Transaction Processing Efficiency	*TPE*	0.2
Margin	*M*	0.1
Waiting Time	*T*	0.1

Similarly, in calculating the reputation of junior notaries, the weight of $PR(j)/L(j)$ is set to 0.4, the weight of $HTSR$ is set to 0.2, the weight of TPE is set to 0.2, and the weight of M is set to 0.1. Additionally, the parameter T, representing the waiting time, is introduced in the reputation calculation for junior notaries, with its weight set to 0.1.

The parameter T is employed to measure the waiting time of a notary node before it becomes a transaction notary. For junior notaries, the opportunities to be selected as transaction notaries and participate in transactions are limited, resulting in longer waiting times. The introduction of parameter T provides junior notaries, who have been part of the notary group for an extended period but lack transaction participation

opportunities, with a prioritized opportunity to advance to intermediate notaries. Simultaneously, it increases the time cost for newly joined malicious nodes within the notary group, reducing the likelihood of such nodes being elected as transaction notaries, thereby enhancing the security of cross-chain operations.

$$T(i)=\frac{T_i - T_{\min}}{T_{\max} - T_{\min}} \tag{6}$$

In Eq. (6), $T_{\max}$ represents the maximum waiting time among all current nodes to become a transaction notary, $T_{\min}$ denotes the minimum waiting time, and $T(i)$ signifies the normalized result of the waiting time for node i.

The improved PageRank algorithm is presented in Eq. (7):

$$PR(i)=\frac{1-d}{N}+d\cdot[0.4\sum_{j\in M(i)}\frac{PR(j)}{L(j)} +0.2HTSR(i)+0.2TPE(i)+0.1M(i)+0.1T(i)] \tag{7}$$

In Eq. (7), $PR(i)$ represents the reputation of node i, N denotes the total number of notary nodes, and d is the damping factor, set at 0.85. $PR(j)$ indicates the reputation of node j, while $L(j)$ signifies the number of nodes evaluated by node j.

C. Hierarchical Management Scheme of the Notary Group

The notary group, based on reputation rankings, employs a normal distribution to classify notary nodes into three levels, as illustrated in Fig. 2: junior notaries, intermediate notaries, and senior notaries.

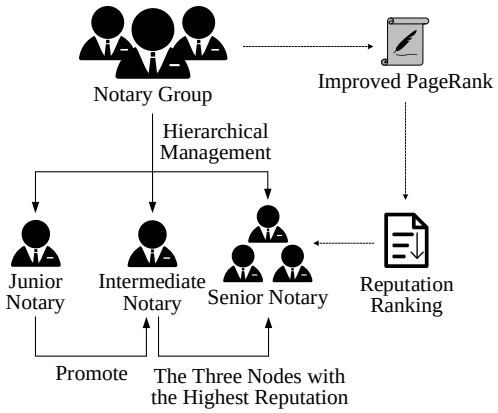


Fig. 2. Hierarchical management scheme of the notary group.

Based on a normal distribution, notary nodes with a reputation less than -1σ are designated as junior notaries, representing the bottom 16% of the notary group in terms of reputation ranking. Notary nodes with a reputation greater than -1σ are classified as intermediate notaries, encompassing the top 84% of the notary group by reputation ranking. Senior notaries are selected as the three nodes with the highest reputation from among the intermediate notaries, corresponding to the three highest-ranked notaries in the entire notary group.

Within the notary group, transaction notaries are preferentially elected from intermediate notaries based on their reputation. Only when no intermediate notary meets the transaction requirements is the same method applied to elect from junior notaries. The promotion of a junior notary to an intermediate notary is contingent upon its reputation. The reputation calculation for junior notaries differs from that of intermediate notaries, notably incorporating the waiting time to become a transaction notary as a significant factor in the evaluation. By appropriately assigning weights, junior notaries with longer waiting times and otherwise favorable attributes achieve higher reputation scores, thereby gaining priority for promotion to intermediate notaries and increasing their opportunities to participate in transactions. The verification of cross-chain transactions is exclusively handled by senior notaries, specifically the three nodes with the highest reputation in the entire notary group, who collectively perform validation through multi-signature processes. Funds are released only after at least two senior notaries have completed their signatures.

D. Hierarchical Notary Election

The hierarchical notary election process is depicted in Fig. 3.

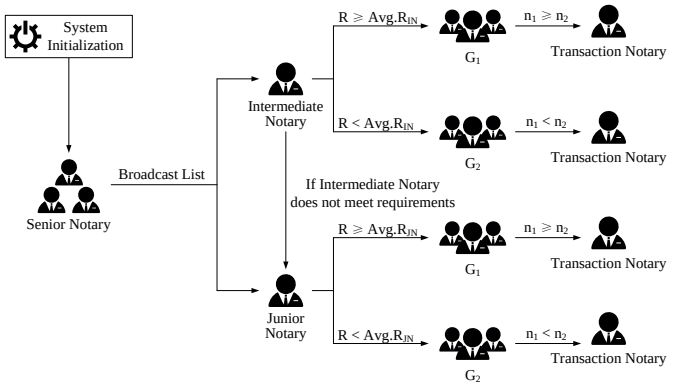


Fig. 3. Hierarchical notary election.

Initially, during the notary initialization phase, the system categorizes each notary into junior notaries, intermediate notaries, and senior notaries based on their reputation. In the preparation stage of a cross-chain transaction, senior notaries broadcast the transaction list within the notary group, detailing the key attributes of the transactions. Each notary then determines whether to participate in the notary election based on the transaction details. Subsequently, the system calculates the average reputation of the intermediate notaries and, based on this mean value, divides them into two groups: G_1, consisting of notaries with a reputation greater than or equal to the average, and G_2, comprising notaries with a reputation below the average. The number of notaries in G_1 is denoted as n_1, and in G_2 as n_2. If $n_1 \geq n_2$, a notary meeting the transaction requirements is elected from G_1 as the transaction notary; otherwise, the same method is applied to elect a

transaction notary from G_2. Should no intermediate notary fulfill the transaction requirements, the system employs the same approach to conduct the election among junior notaries. The specific procedure is outlined in Algorithm 1.

Algorithm 1: Notary Election

Input: $List_{TRA}$, Tab_R, IN, JN

Output: TN

```
function ELECTION( List_TRA , Tab_R , IN , JN )
  Broadcast( List_TRA )
  R ← DeleteZeroReputationNotary( Tab_R )
  TN ← Elect( IN )
  Avg.R ← Average( R )
  G_1 ← GetIN( R ≥ Avg.R ), n_1 = Count( G_1 )
  G_2 ← GetIN( R < Avg.R ), n_2 = Count( G_2 )
  if n_1 ≥ n_2 then
    TN ← Random( G_1 )
  else if n_1 < n_2 then
    TN ← Random( G_2 )
  else if TN ← Null( IN ) then
    return Elect( JN )
  end if
  return TN
end function
```

IV. Performance Analysis

The simulation experimental environment for this scheme is executed on a laptop equipped with the Windows 11 operating system, featuring hardware specifications that include a 13th-generation Intel(R) Core(TM) i5-13500H 2.60 GHz processor and 16 GB RAM. The blockchain system is constructed within a virtual machine running Ubuntu 24.04 Desktop Edition, configured with a 4-core processor and 8 GB RAM. The blockchain system utilized in the experiments is based on Hyperledger Fabric 2.4, comprising two independent blockchains with identical configurations.

A. Election Performance of the Improved PageRank Algorithm

This experiment constructs a notary group comprising 50 nodes. During initialization, each node is assigned a uniform initial reputation of 0.02 and numbered from 1 to 50. Nodes numbered 1 to 3 are preconfigured with a higher density of trust relationships and are designated as senior notary nodes in the HMNG-CCM framework; nodes numbered 4 to 42 are configured with baseline trust relationships and defined as intermediate notary nodes; and newly added nodes numbered 43 to 50, lacking pre-established trust relationships, are classified as junior notary nodes. Throughout the iteration process, the establishment of trust relationships is determined by the current reputation of each node, with the probability of a node gaining new trust relationships being positively correlated with its current reputation. The iteration concludes when the reputation of each node stabilizes, with the resulting reputation values for each node presented in Fig. 4.

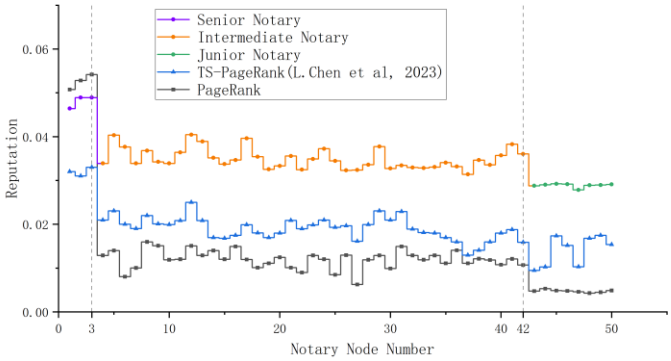


Fig. 4. Results of the PageRank, TS-PageRank, and HMNG-PageRank.

The original PageRank algorithm, due to its excessive reliance on trust relationships, results in nodes numbered 1 to 3 (mean: 0.052) exhibiting significantly higher reputation scores than nodes numbered 4 to 42 (mean: 0.012) and nodes numbered 43 to 50 (mean: 0.0048). This approach overlooks the complexity of notary reputation evaluation in cross-chain transactions, leading to a one-sided assessment of reputation. In contrast, the TS-PageRank [36] algorithm, when computing the reputation of notary nodes, incorporates parameters that may influence node reputation in cross-chain transactions, partially mitigating the short-comings of the original PageRank algorithm. However, it demonstrates insufficient differentiation between nodes numbered 4 to 42 and those numbered 43 to 50, which may result in the erroneous election of newly joined malicious nodes as transaction notaries during the notary selection process, consequently reducing system security.

HMNG-CCM designs differentiated reputation evaluation strategies for junior and intermediate notaries. Consequently, the reputation of senior, intermediate, and junior notaries, computed via the improved HMNG-PageRank algorithm, exhibits a discernible level of differentiation while achieving a smooth transition from senior to junior levels. This approach avoids the steep drop-off observed in the original PageRank algorithm and the flat distribution of the TS-PageRank algorithm, ensuring a comprehensive reputation assessment. Furthermore, the differentiated evaluation strategy demonstrates a high degree of adaptability to the hierarchical requirements of notary elections, whereas the original PageRank and TS-PageRank algorithms, lacking similar designs, exhibit limitations under complex trust relationship scenarios.

In summary, the HMNG-PageRank algorithm excels in reputation evaluation within the notary group. Compared to the original PageRank and TS-PageRank, this scheme offers superior reliability and security, providing robust support for the hierarchical notary election mechanism.

B. Comparison of Notary System Time Cost and Cross-Chain Transaction Time

This experiment analyzes the time cost of each phase in cross-chain transactions, testing the average time costs of the

preparation phase, transaction phase, confirmation phase, and notary system under scenarios involving the simultaneous initiation of 20, 40, 60, 80, 100, and 120 transactions. The experimental results are presented in Fig. 5. The preparation phase accounts for approximately 37.1% of the total time cost in the cross-chain transaction process, the transaction phase constitutes about 47.5%, and the confirmation phase comprises roughly 15.4%. The time cost of the notary system, which forms a subset of the preparation phase, represents approximately 4.5% of the total time cost. The proportion of time attributed to the notary system is significantly lower than that of the entire cross-chain transaction process, indicating that the additional time overhead introduced by the notary management scheme is negligible. Furthermore, as the number of transactions increases from 20 to 120, the average cross-chain transaction time rises by only 4.6%, demonstrating the efficiency of HMNG-CCM in resource allocation and its adaptability to varying transaction scales.

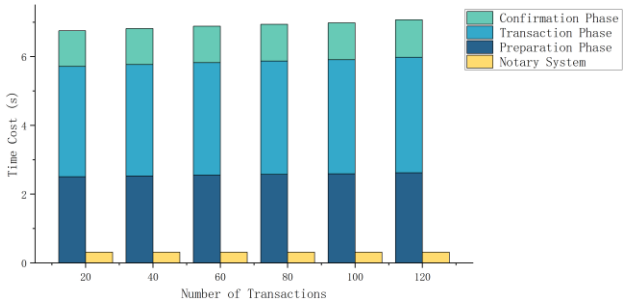


Fig. 5. Notary system time cost and cross-chain transaction time.

C. Impact of Malicious Nodes on Cross-Chain Transaction Time

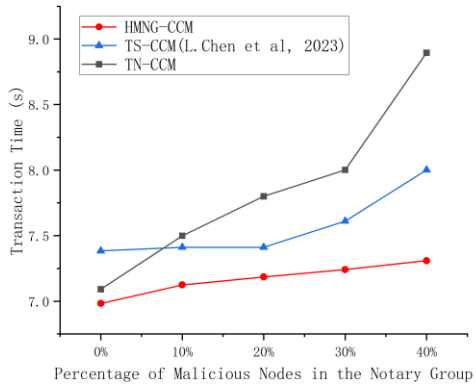
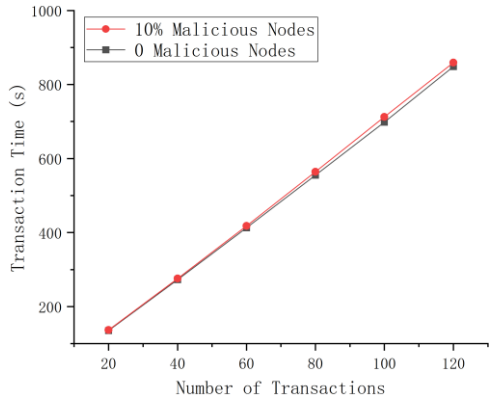


Fig. 6. Transaction time under different percentages of malicious nodes.

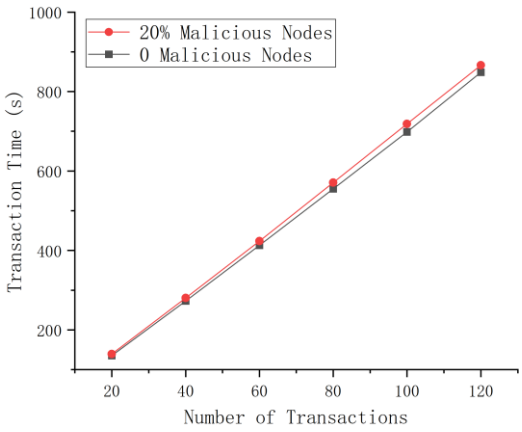
This experiment initiates 100 transaction requests to evaluate cross-chain transaction times when the notary group contains 0, 10%, 20%, 30%, and 40% malicious nodes. The experimental results are presented in Fig. 6. The Traditional Notary Cross-Chain Mechanism (TN-CCM) exhibits low tolerance to malicious nodes. As the proportion of malicious nodes increases, the cross-chain transaction time consistently rises. Notably, when the proportion of malicious nodes exceeds 30%, the transaction time surges to 8.9 seconds, representing a time cost increase of approximately 25.4%, which indicates a marked degradation in system performance.

The Three-Stage Cross-Chain Mechanism (TS-CCM) [36], operates normally when the proportion of malicious nodes remains below 20%, with transaction times stabilized at approximately 7.4 seconds. However, when the proportion of malicious nodes exceeds 20%, transaction time increase sharply to 8 seconds, resulting in an approximate time cost rise of 8.4%, with further escalation as the proportion of malicious nodes continues to grow. This indicates that TS-CCM experiences significant impacts on its performance and stability when confronted with higher proportions of malicious nodes.

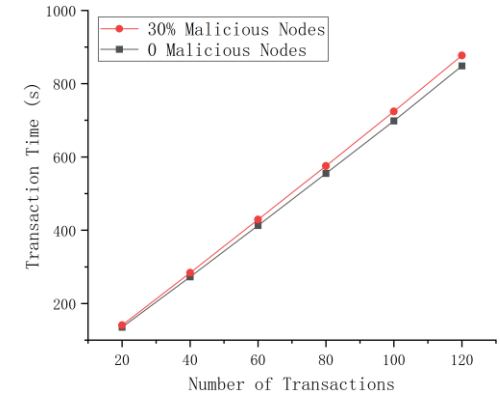
Throughout the range of 0% to 40% malicious nodes, HMNG-CCM consistently demonstrates lower cross-chain transaction times compared to TN-CCM and TS-CCM. Moreover, as the proportion of malicious nodes increases, the growth in transaction time for HMNG-CCM remains relatively minor. Specifically, when the proportion of malicious nodes reaches 40%, the transaction time increases by only 4.67%, demonstrating its robustness and resistance to malicious behavior. In summary, the experimental results comprehensively validate that HMNG-CCM not only maintains high efficiency when the proportion of malicious nodes is low, but also sustains stable system performance under scenarios with a high proportion of malicious nodes. This reflects the significant engineering value of HMNG-CCM in enhancing the efficiency and reliability of cross-chain transactions.



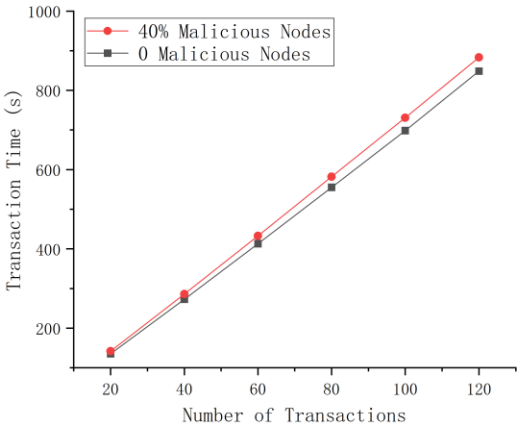
(a) 10% Malicious Nodes



(b) 20% Malicious Nodes



(c) 30% Malicious Nodes



(d) 40% Malicious Nodes

Fig. 7. Impact of different percentages of malicious nodes on transaction time under different numbers of transactions.

This experiment evaluates the performance of HMNG-CCM in counteracting malicious notary nodes during cross-chain transactions. The experiment simulates five scenarios with malicious notary proportions of 0% (control group), 10%, 20%, 30%, and 40%. For each scenario, 20, 40, 60, 80, 100, and 120 transactions are processed, analyzing the impact of both transaction volume and malicious notary proportion on transaction time. The experimental results are presented in Fig. 7. In the absence of malicious nodes (0%), cross-chain transaction times are the shortest, exhibiting linear growth with increasing transaction volume. As the proportion of malicious nodes rises from 10% to 40%, transaction time increases slightly compared to the 0% malicious notary scenario, as evidenced by the gradually widening vertical distance between the corresponding line segments and the 0% malicious notary baseline in the figure. Nevertheless, even when the malicious notary proportion reaches 40%, transaction times remain closely aligned with those in the 0% scenario. This demonstrates that HMNG-CCM sustains robust performance even under high proportions of malicious nodes. Furthermore, regardless of the increase in transaction volume, the influence of varying malicious notary proportions on transaction time remains limited, highlighting the efficiency and robustness of HMNG-CCM in mitigating interference from malicious nodes.

D. Impact of Malicious Nodes on Transaction Success Rate

This experiment initiates 100 transaction requests to assess the cross-chain transaction success rate under scenarios where the notary group contains malicious nodes at proportions of 10%, 20%, 30%, and 40%. The experimental results are presented in Fig. 8. TN-CCM exhibits low tolerance to malicious behavior; as the proportion of malicious nodes increases, the transaction success rate declines linearly from 100% to 60%. This indicates that TN-CCM struggles to maintain normal system operation effectively when the proportion of malicious nodes is high. TS-CCM [36], performs stably when the malicious notary proportion is below 30%, maintaining a transaction success rate of 98%. However, when the proportion exceeds 30%, the success rate drops sharply to 88%, highlighting its limited resilience against malicious behavior in high-risk scenarios.

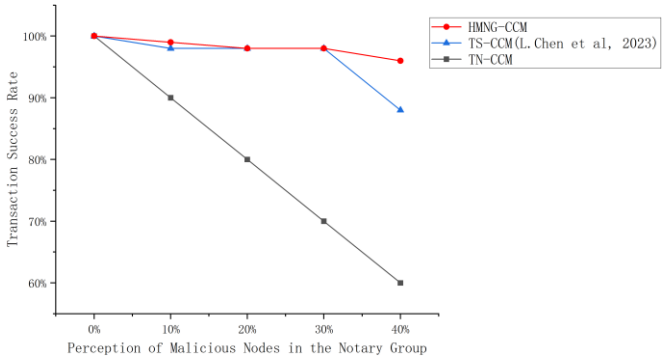


Fig. 8. Transaction success rate under different percentages of malicious nodes.

In contrast, HMNG-CCM achieves a transaction success rate of 99% when the malicious notary proportion is below 20%, slightly outperforming TS-CCM. Between 20% and 30%, the success rate remains stable at 98%. Even when the malicious notary proportion reaches 40%, HMNG-CCM sustains a success rate of 96%, with a mere 4% decline, markedly surpassing both TN-CCM and TS-CCM. These results demonstrate that HMNG-CCM effectively ensures transaction success rates in scenarios with high proportions of malicious nodes, reflecting superior system reliability and robustness under complex scenarios.

E. Security Analysis

The notary-based cross-chain transaction system may encounter threats such as malicious notary attacks, single points of failure, and reputation manipulation. The HMNG-CCM proposed in this paper effectively addresses these potential threats and ensures system robustness and reliability through an innovative hierarchical notary management scheme, a functional division mechanism, and a reputation evaluation mechanism based on an improved PageRank algorithm.

The core of HMNG-CCM lies in mitigating trust risks and enhancing system stability through hierarchical management and functional division. Notaries are classified into three tiers—junior, intermediate, and senior. Nodes newly joining the notary group must stake a margin deposit and undergo

verification by senior notaries to become junior notaries, while senior notaries are designated as the nodes with the highest reputation. This hierarchical structure circumvents the centralization risks inherent in traditional notary mechanisms due to reliance on a single notary. The synergy between functional division and hierarchical management enhances the system's decentralization. Transaction execution and verification duties are distinctly separated: junior and intermediate notaries handle the execution of cross-chain transactions, whereas senior notaries focus on verifying the legality and consistency of transactions. This division further diminishes the influence of any single notary on the system, while enabling the timely detection and correction of malicious behavior through multiple checks. Consequently, the system maintains normal operation even in the presence of partial node failures or attacks.

The reputation evaluation employs an improved PageRank algorithm, generating reputation rankings based on nodes' historical performance and trust relationships. Differentiated evaluation strategies are designed for junior and intermediate notaries to reflect their distinct role characteristics in transaction execution. Periodically updated reputation rankings effectively identify and isolate malicious nodes, ensuring that only those with a high reputation participate in critical tasks. This dynamic adjustment capability not only prevents reputation manipulation but also provides a fair basis for notary election and promotion. When junior notaries are considered for promotion to intermediate notaries, both historical performance and waiting time are comprehensively evaluated, offering priority promotion opportunities to junior notary nodes that have been part of the notary group for an extended period yet lack election opportunities. Simultaneously, this approach increases the time cost for newly joined malicious nodes within the notary group, reducing the likelihood of their election as selected notaries and thereby further mitigating their impact on the system.

Based on the aforementioned design, this scheme ensures transaction security and smooth execution through a cross-chain protocol. During the preparation phase, the system selects transaction notaries from intermediate or junior notaries based on reputation. In the transaction phase, senior notaries verify transactions via multi-signature validation and authorize transaction notaries to release funds, a decentralized verification approach that effectively prevents single points of failure. Furthermore, the system incorporates timeout and retry mechanisms to bolster risk resilience and employs distributed storage technology in the confirmation phase to safeguard transaction data security. Collectively, these design elements establish a secure and reliable transaction process.

V. Conclusion

The HMNG-CCM proposed in this paper provides a decentralized, efficient, and trustworthy solution for blockchain cross-chain transactions by introducing an innovative notary management scheme, a functional division mechanism, and a reliable reputation evaluation mechanism.

Firstly, a notary management scheme centered on hierarchical management and functional division effectively mitigates trust risks and optimizes transaction processes, thereby enhancing the decentralization characteristics of the cross-chain system. Secondly, a reputation evaluation scheme designed using an improved PageRank algorithm implements differentiated assessments based on notary levels, ensuring fairness and rationality in the evaluation process. Furthermore, experimental results conducted on the Hyperledger Fabric platform demonstrate that this mechanism effectively withstands malicious notary behavior while improving transaction speed and success rate, confirming its advantages in practical applications.

Although this study has achieved significant progress, several limitations warrant further attention. The experimental validation is primarily based on the Hyperledger Fabric platform, and the generalizability of the results requires additional verification across other blockchain platforms. The hierarchical management scheme may increase management complexity when the number of notaries is large. Furthermore, the effectiveness and stability of the reputation evaluation scheme under diverse scenarios necessitate further testing.

Based on the findings and limitations of this study, future research could explore adaptive dynamic management schemes for notary groups, incorporate machine learning techniques to develop more flexible reputation evaluation models, and design cross-chain protocols that support multi-chain environments to accommodate increasingly complex blockchain interaction scenarios.

In conclusion, this paper successfully establishes an efficient and secure cross-chain mechanism, offering robust technical support for the security and decentralization of blockchain cross-chain transactions. While certain limitations remain, this study provides directions for future related research, bearing significant theoretical importance and practical value.

Acknowledgment

Funding Statement: This research was funded by the Jilin Provincial Department of Education Scientific Research Project (Project No. JJKH20250872KJ). The funding body had no role in the design of the study, collection, analysis, and interpretation of data, or in writing the manuscript.

References

[1] Atlam HF, Ekuri N, Azad MA, Lallie HS, "Blockchain forensics: A systematic literature review of techniques, applications, challenges, and future directions," Electronics, vol. 13, no. 17, p. 3568, 2024, doi: 10.3390/electronics13173568.

[2] Nakamoto S, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, vol., no., p. 21260, 2008.

[3] Buterin V, "A next-generation smart contract and decentralized application platform," White Paper, vol. 3, no. 37, pp. 2-1, 2014.

[4] Sharma M, Sharma M, Rawat B, "Impact of blockchain technology on financial services," 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Tandojam, Pakistan, pp. 1-6, 2024, doi: 10.1109/KHI-HTC60760.2024.10482252.

[5] Qu ZG, Meng YY, Liu B, Muhammad G, Tiwari P, "QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT," IEEE Internet of Things Journal, vol. 11, no. 1, pp. 40-49, 2024, doi: 10.1109/jiot.2023.3285388.

[6] Rejeb A, Rejeb K, Appolloni A, Jagtap S, Iranmanesh M, Alghamdi S, et al., "Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions," Internet of Things and

Cyber-Physical Systems, vol. 4, no., pp. 1-18, 2024, doi: 10.1016/j.iotcps.2023.06.003.

[7] Zhu S, Chi C, Liu Y, "A study on the challenges and solutions of blockchain interoperability," China Communications, vol. 20, no. 6, pp. 148-165, 2023, doi: 10.23919/JCC.2023.00.026.

[8] Xue L, Liu DX, Huang C, Shen XM, Zhuang WH, Sun R, Ying BD, "Blockchain-based data sharing with key update for future networks," IEEE Journal on Selected Areas in Communications, vol. 40, no. 12, pp. 3437-3451, 2022, doi: 10.1109/jsac.2022.3213312.

[9] Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," Proceedings of the Thirteenth EuroSys Conference, pp. 1-15, 2018.

[10] Zhou Y, Bai Y, Liu Z, Gao H, Liu C, Lei H, "Exploring cross-chain mechanisms and projects in blockchain: A comprehensive summary," Proceedings of the 13th International Conference on Computer Engineering and Networks Lecture Notes in Electrical Engineering (1125), pp. 421-431, 2024, doi: 10.1007/978-981-99-9239-3_41.

[11] Augusto A, Belchior R, Correia M, Vasconcelos A, Zhang LY, Hardjono T, Ieee Computer SOC, "SoK: Security and privacy of blockchain interoperability," 45th IEEE Symposium on Security and Privacy (SP), San Francisco, CA, pp. 3840-3865, 2024, doi: 10.1109/sp54263.2024.00255.

[12] Wang J, Wan Y, Hu Y, Yuan Y, Fan K, "Cross-chain supervision mechanism of distributed notaries for consortium blockchain," 2023 6th International Conference on Artificial Intelligence and Big Data (ICAIBD), pp. 579-584, 2023, doi: 10.1109/icaibd57115.2023.10206042.

[13] Li B, Duan TT, Zhao QL, Guo Y, Song ZX, Zhang HW, et al., "Performance modeling of relay chain," IEEE/ACM Transactions on Networking, vol. 33, no. 1, pp. 194-209, 2024, doi: 10.1109/tnet.2024.3487935.

[14] Wang YL, Chen Z, Ma RH, Ma B, Xian YJ, Li Q, "Toward a secure and private cross-chain protocol based on encrypted communication," Electronics, vol. 13, no. 16, 2024, doi: 10.3390/electronics13163116.

[15] Dehez-Clementi M, Lacan J, Deneuville JC, Asghar H, Kaafar D, "A blockchain-enabled anonymous-yet-traceable distributed key generation," 2021 IEEE International Conference on Blockchain (Blockchain), pp. 257-265, 2021, doi: 10.1109/Blockchain53845.2021.00042.

[16] Duan TT, Zhang HW, Li B, Song ZX, Li ZC, Zhang J, Sun Y, "Survey on blockchain interoperability," Journal of Software, vol. 35, no. 2, pp. 800-827, 2024, doi: 10.13328/j.cnki.jos.006950.

[17] Zhang YS, Jiang JJ, Dong XW, Wang LM, Xiang Y, "BeDCV: blockchain-enabled decentralized consistency verification for cross-chain calculation," IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 2273-2284, 2023, doi: 10.1109/tcc.2022.3196937.

[18] Wei W, Zhou Y, Li D, Hong X, "Double-layer blockchain-based decentralized integrity verification for multi-chain cross-chain data," Neural Information Processing: 30th International Conference, ICONIP 2023, Proceedings Lecture Notes in Computer Science (14452), pp. 264-279, 2024, doi: 10.1007/978-981-99-8076-5_19.

[19] Wu O, Huang B, Li S, Wang Y, Li H, "A performance evaluation method for a class of cross-chain systems," Mobile Networks and Management: 12th EAI International Conference, MONAMI 2022, Virtual Event, Proceedings Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (474), pp. 265-281, 2023, doi: 10.1007/978-3-031-32443-7_19.

[20] Duan L, Sun YY, Ni W, Ding WP, Liu JQ, Wang W, "Attacks against cross-chain systems and defense approaches: A contemporary survey," IEEE/CAA Journal of Automatica Sinica, vol. 10, no. 8, pp. 1647-1667, 2023, doi: 10.1109/jas.2023.123642.

[21] Hou Q, Wang Q, Chen X, "Design and optimization of heterogeneous blockchain network model based on relay chain," 2023 16th International Conference on Advanced Computer Theory and Engineering (ICACTE), pp. 1-5, 2023, doi: 10.1109/icacte59887.2023.10335272.

[22] Wang HN, Wang JY, Liu LX, Lu Y, "Temporary relay: A more flexible way to cross chains," Peer-to-Peer Networking and Applications, vol. 17, no. 5, pp. 3489-3504, 2024, doi: 10.1007/s12083-024-01762-3.

[23] Wu C, Wang J, Xiong H, Yi W, Zhao Y, "A secure cross-chain mechanism based on relay chain and smart contract encryption scheme," 2023 11th International Conference on Information Systems and Computing Technology (ISCTech), pp. 87-91, 2023, doi: 10.1109/ISCTech60480.2023.00023.

[24] Wang KY, Jia LP, Song ZX, Sun Y, "Mitosis: A scalable sharding system featuring multiple dynamic relay chains," IEEE Transactions on Parallel and Distributed Systems, vol. 35, no. 12, pp. 2497-2512, 2024, doi: 10.1109/tpds.2024.3480223.

[25] Li Y, Tuo W, Hu Q, Ma L, "A novel cross-chain relay method based on node trust evaluation," Tools for Design, Implementation and Verification of Emerging Information Technologies: 18th EAI International Conference, TRIDENTCOM 2023, Proceedings Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering (523), pp. 3-20, 2024, doi: 10.1007/978-3-031-51399-2_1.

[26] Li J, Zhao WT, "Blockchain cross-chain protocol based on improved Hashed Time-Locked Contract," Cluster Computing-the Journal of Networks Software Tools and Applications, vol. 27, no. 9, pp. 12007-12027, 2024, doi: 10.1007/s10586-024-04537-w.

[27] [27] Wang K, Wang D, Zhi H, Chen Y, Zhang X, "Hash time lock with dynamic premium based on credit in cross-chain transaction," 2024 IEEE International Conference on Blockchain (Blockchain), pp. 123-130, 2024, doi: 10.1109/Blockchain62396.2024.00025.

[28] Yu B, Guan Y, Geng S, Miao L, Zhang Y, Gong Y, "A blockchain-enhanced secure and reliable data transaction scheme in MAS via HTLC," 2024 3rd Conference on Fully Actuated System Theory and Applications (FASTA), pp. 494-499, 2024, doi: 10.1109/fasta61401.2024.10595264.

[29] Barbàra F, Schifanella C, "MP-HTLC: Enabling blockchain interoperability through a multiparty implementation of the Hash Time-Lock Contract," Concurrency and Computation-Practice & Experience, vol. 35, no. 9, 2023, doi: 10.1002/cpe.7656.

[30] Yu Y, Li Z, Tu Y, Yuan Y, Li Y, Pang Z, "Blockchain-based distributed identity cryptography key management," 2023 15th International Conference on Computer Research and Development (ICCRD), pp. 236-240, 2023, doi: 10.1109/iccrd56364.2023.10080490.

[31] Zhao XF, Peng CG, Tan WJ, Niu K, "Blockchain-based key management scheme using rational secret sharing," CMC-Computers Materials & Continua, vol. 79, no. 1, pp. 307-328, 2024, doi: 10.32604/cmc.2024.047975.

[32] Ren ZX, Yu YM, Yan EH, Chen TW, "L2-MA-CPABE: A ciphertext access control scheme integrating blockchain and off-chain computation with zero knowledge proof," Journal of King Saud University-Computer and Information Sciences, vol. 36, no. 10, 2024, doi: 10.1016/j.jksuci.2024.102247.

[33] Hope-Bailie A, Thomas S, "Interledger: Creating a standard for payments," Proceedings of the 25th International Conference Companion on World Wide Web, pp. 281-282, 2016.

[34] Xiong A, Liu G, Zhu Q, Jing A, Loke SW, "A notary group-based cross-chain mechanism," Digital Communications and Networks, vol. 8, no. 6, pp. 1059-1067, 2022, doi: 10.1016/j.dcan.2022.04.012.

[35] Chen KH, Lee LF, Chiu W, Su CH, Yeh KH, Chao HC, "A trusted reputation management scheme for cross-chain transactions," Sensors, vol. 23, no. 13, p. 6033, 2023, doi: 10.3390/s23136033.

[36] Chen LF, Yao ZY, Si XM, Zhang Q, "Three-stage cross-chain protocol based on notary group," Electronics, vol. 12, no. 13, p. 2804, 2023, doi: 10.3390/electronics12132804.