Wang et al. *EPJ Quantum Technology* (2026) 13:23
https://doi.org/10.1140/epjqt/s40507-025-00462-y

EPJ.org

EPJ Quantum Technology

RESEARCH Open Access

A cross-chain model with underlying security and scalability based on quantum algorithm

Zhuo Wang[1,2], Jian Li[2*], Ang Liu[3], Mianxiong Dong[4] and Yanyan Hou[5]

*Correspondence:
lijian@bupt.edu.cn
[2]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, 100876, China
Full list of author information is available at the end of the article

Abstract

Cross-chain relay architectures face critical security gaps: centralized trust dependencies, consensus vulnerabilities, and potential quantum threats. We propose the Quantum Cross-Chain (QCC) model—a post-quantum secure framework integrating quantum cryptography at the foundational layer. QCC establishes a global identity registry for heterogeneous chains and introduces a Two-Way Identity Authentication (TIA) protocol using GHZ entanglement, enabling information-theoretically secure mutual verification in a single execution. To fortify transaction integrity, we design a Quantum Ring Signature (QRS) scheme with novel key-loss security, ensuring that compromised keys cannot forge valid signatures. Unlike conventional systems that rely on smart contract autonomy, QCC delegates security to quantum one-way functions and distributed auditing, synchronizing consensus transmission with cryptographic validation. Formal verification proves composite security bounded by $\mathbf{negl}(n) + \mathbf{negl}(q)$, while simulations demonstrate stable throughput (78.5 TPS) and predictable latency (130 ms) under variable network conditions. QCC achieves post-quantum resilience, decentralized auditability, and linear scalability, providing a practical blueprint for next-generation cross-chain infrastructure.

Keywords: Cross-chain; Access control; Quantum signature; Secure mechanism

1 Introduction

Since the advent of the cryptocurrency Bitcoin in 2008, its underlying technology, the blockchain, has been emerged [1]. Blockchain technology has flourished, finding applications in numerous scenarios, and various blockchain systems have been constructed to meet specific needs [2]. However, each blockchain is specialized to meet specific requirements in the application. These blockchains vary in permission type, consensus mechanism, smart contract, data structure, etc. The data and assets in one blockchain cannot interconnect with another blockchain. The cross-chain technology bridges the gap between independent application blockchains to eliminate "information islands" and realize interconnectivity and interoperability across different blockchain networks. In recent

Springer

years, scholars have provided various feasible solutions to solve cross-chain data interactions [3, 4]. A cross-chain network effectively breaks down barriers between institutions and opens pathways to enable data flow and value circulation between application chains.

The relay chain, such as RootStock and Cosmos, combines the side chain and notary [5]. It is a scalable solution that verifies transactions by the application chain. A *relay* is an independent cross-chain operation layer abstractly separated from an application chain. A relay uses a global language, enabling cross-chain transactions between two heterogeneous application chains.

However, the current relay chain solution faces some practical problems. In recent years, to perform necessary data interactions and asset transfers during cross-chain transactions, the cross-chain network poses security issues such as privacy leakage and loss of property [6]. An attack by malicious users cost the Value DeFi protocol $6 million on November 15, 2020 [7]. The PolyNetwork protocol was said to have been attacked on August 10, 2021, due to key leakage. This led to the theft of over $610 million [8] and the compromise of a significant amount of private user data. Therein, Security breaches may originate from inadequate authentication mechanisms within the relay network, allowing malicious users to exploit leaked keys and impersonate legitimate relay nodes. The key leakage may be caused by the insecure key generation and distribution mechanism, or the key could be breached by an adversary with large amounts of computing resources or force majeure.

In a relay cross-chain scheme, a typical cross-chain transaction is completed with three transactions recorded in the initiator, destination, and relay chains, respectively. After receiving the block output information from the initiator chain, the relay node verifies the block, resolves the cross-chain transaction in the block, and generates the cross-chain transaction. The relay nodes sign according to the chain consensus mechanism, and package cross-chain transactions during block output. The cross-chain process, like Cosmos [9] and Polkadot [10], typically requires the assistance of a third party because the interaction between heterogeneous application chains is complicated. Therefore, cross-chain security depends on the reliability and security of the relay chain, which can eliminate illegal user access, malicious users' forgery, key leakage, and forgery caused by key-loss. This requires higher security for the cross-chain mechanism. However, at present, the interaction between the relay chain and the application chain is in a centralized manner, and the execution of transactions relies on the development and support of the smart contract of the relay chain. From the security point of view, the implementation of functions in the upper layer needs to consider not only the completeness of its own business logic, but also the attacks from the underlying system, and the vulnerability of the underlying system will also have a greater impact on the security of the upper layer applications. Therefore, it is more effective to enforce the security of cross-chain mechanisms on cryptographic algorithms than on the autonomous capabilities of relay chains or smart contracts. For example, monitoring the malicious behavior of intermediaries requires deploying smart contracts, nevertheless, placing the monitoring mechanism in the underlying cryptographic algorithm will improve the reliability of the relay chain.

Meanwhile, as the consensus mechanism, signature algorithm, and identity authentication applied to a cross-chain transaction are based on computational complexity, they are vulnerable to quantum attacks [11–13]. Numerous researchers have proposed various interaction models to address the post-quantum blockchain's quantum security and cross-chain data interaction security issues. Lee et al. [14] proposed a blockchain-based

settlement model that uses executable cross-chain atomic swaps for digital currency. Their model adopts a third-party administrative blockchain for failure reduction and efficiency improvement while a lattice-based aggregate signature is deployed for post-quantum security. However, the management's dependence on third parties leads to a high degree of centralization. The limitations of cross-chain atomic swaps, such as slowness, inefficiency, and high cost, may hinder their practicality in actual applications [15]. In 2022, Cui et al. [16] proposed a cross-chain protocol that uses a quantum time lock based on quantum cryptography to guarantee the atomicity of cross-chain asset exchanges and uses an identity information chain to provide users in consortium blockchains with identity validation. However, their cross-chain transaction security only relies on the time lock in the smart contract layer, it risks disputes arising easily from inconsistent transaction records due to the lack of a consensus transfer process between the two application chains. Currently, the cross-chain mechanism aims to solve the cross-chain issues in trust, consensus, security, and network. And its main technical solutions mainly focus on key security, identity authentication security, cross-chain consensus security and transaction verification capability [17].

There are some recent studies that address relay-based challenges through innovative cryptographic techniques and relay chain architectures. Qu et al. [18] proposed a supply chain-driven quantum blockchain cross-chain scheme (SCS-QBCT) that uses quantum Fourier transform (QFT) to compress transaction records on relay chains, reducing storage loads. A multifunctional smart contract handles value transfer and queries, with experiments showing low gas consumption and latency. Yu and Huang [19] designed an anti-quantum cross-chain identity authentication approach (DGS-AQCCIDAA) for smart education, using dynamic group signatures based on lattice problems (LWE and ISIS). The relay chain model ensures anonymity and traceability, with performance tests indicating lower computational overhead than existing schemes. Limitations include potential latency in large-scale deployments. Zhang et al. [20] developed a cross-chain asset transaction method leveraging ring signatures to hide user identities. The RCROSS contract integrates ring signatures with relay technology, providing resistance to replay and man-in-the-middle attacks. Gas consumption tests show practicality, but increased ring members raise costs and latency. Li et al. [21] introduced a cross-chain privacy-preserving (CCPP) model for BIoMT, using a designated verifier proxy signature (DVPS) based on lattice theory. The relay chain facilitates medical data sharing, while DVPS ensures unforgeability and nontransferability. Evaluations demonstrate stable throughput ($\sim$1000 TPS) but higher energy consumption due to lattice operations.

This paper proposes a quantum relay chain model (QCC) providing access control and a secure cross-chain solution. Classical public-key signatures are discarded to circumvent quantum computing attack threats [22]. The QCC introduces a relay chain to perform identity authentication and transaction execution in cross-chain network. In QCC, a two-way identity authentication protocol (TIA) and a quantum ring signature (QRS) are deployed. As a quantum cryptography technology, the QRS offers robustness for QCC to improve cross-chain mechanism security and cross-chain consensus transmission. The TIA protocol based on GHZ particles is adopted for two-way identity authentication, which can ensure communication security and cross-chain node legitimacy. In addition, the PoA consensus mechanism is utilized in QCC to increase the efficiency of the relay chain in

processing cross-chain transactions and to establish trust between the initiator and the receiver in a cross-chain transaction.

The following are the main contributions of this paper:

1) By the advantages of quantum cryptography in security, this paper proposes the QCC model to improve transaction security for cross-chain applications. The model has post-quantum security and algorithm-supported scalability.
2) Access control. It presents a global cross-chain identity entry solution for heterogeneous application chains. The TIA protocol is adopted to achieve secure two-way authentication, limiting the participation of spurious relay nodes and illegal users to enhance security. The protocol needs to be executed only once to accomplish the identity authentication of both sides, improving the processing efficiency of cross-chain transactions.
3) Secure cross-chain solution. By developing a QRS with key-loss security and auditability, QCC achieves information integrity, reliability of relay, decentralization of the relay chain, and cross-chain consensus transmission. The security of the cross-chain mechanism is improved by the underlying cryptographic algorithm of QCC.

This paper is organized as follows: Sect. 2 details the quantum relay chain scheme. Section 3 introduces QCC's identity registration and authentication features. In Sect. 4, the QCC scheme's transaction execution is explained. In Sect. 5, the security analysis of QCC is presented. Section 6 covers the scalability of QCC, and Sect. 7 gives a conclusion.

2 The model framework

A cross-chain transaction entity comprises two application chains and a relay chain.

Application chain: After satisfying the identity authentication of the relay chain, it can interact with other application chains in the cross-chain network as participants in cross-chain transactions. An application chain can only access the cross-chain system after registering in the relay chain. Each application chain has a built-in manager node that issues identification to each valid node (user) of the application chain and updates the ID and the corresponding address in the relay chain in real time.

Quantum Relay chain (QRC): A relay network with quantum capabilities and devices such as quantum communication, quantum registers, etc. Digital identity management, application chain management, cross-chain transaction verification and upkeep all use the relay chain. As a third party, the relay chain acts as the identity authority center to perform identity registration for application chains. The application chain must register its identity on the relay chain to apply for access to the cross-chain system. The relay chain serves as a cross-chain trust transfer service mechanism and a verification and forwarding facility for cross-chain transactions.

After the application chain submits a cross-chain transaction request, QCC will initiate the identity authentication and execute the cross-chain transaction. The relay chain stores the application chain's ID, each valid user's ID and its corresponding address, and conducts cross-chain transactions based on this. The relay chain can query the destination chain's address by searching on the distributed hash table (DHT) according to the user's request and forward the transaction to the destination chain.

When cross-chain transactions are carried out in the relay chain, there are three types of nodes responsible for transaction issuance, among which, the ordinary node is responsible for identity authentication, review, and issuance of transactions; validating node is

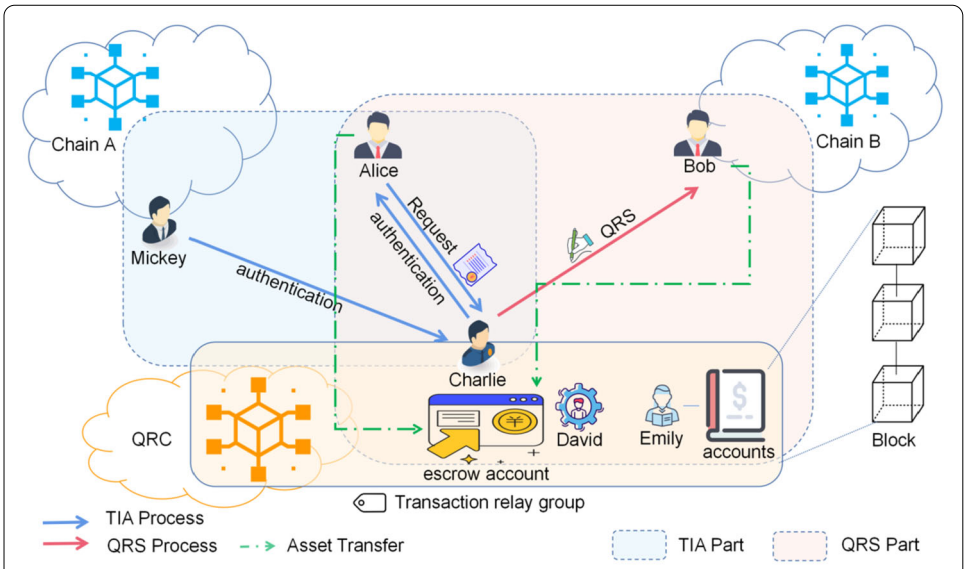

Figure 1 Illustration of a cross-chain transaction in the QCC model

responsible for transaction audit, and the leader node is responsible for bookkeeping in QCC. Generally, validating nodes have published their identity publicly and are authorized by the relay chain with a strict audit procedure before they obtain the authority to become validating nodes. In order to improve the efficiency of leadership node election in QRC and meet the adaptability requirements of leadership node, proof of authority (POA) is used as consensus mechanism in the model.

2.1 Cross-chain transaction process

For simplicity, an example in which two application chains transact through QCC is described in the main part of this paper, as shown in Fig. 1. Suppose Alice buys one of Bob's marketable Non-Fungible Token (NFT) for a certain amount of digital currency. Alice in chain A initiates a cross-chain transaction request with Bob in chain B. The manager node of chain A is Mickey, and Charlie is an ordinary node in the relay chain C processing the transaction request. David is a validating node in chain C, and Emily is the leader node in chain C.

Step 1 Alice generates a cross-chain transaction list. The list contains the initiator: Alice's ID, the destination user: Bob's ID, the number of assets, the accounts in chain A and B, the timestamp, and other essential information. Alice sends the cross-chain request with the list to Charlie.

Step 2 Charlie receives the request, and the contract layer initiates the TIA protocol. If the identity authentication of Alice and Charlie succeeds, the transaction request is permitted. Alice transfers assets to Charlie and generates a transaction record in the list. Otherwise, the transaction will terminate.

Step 3 Charlie receives Alice's asset by an escrow account, puts the asset into the pool of funds, and sets a time lock for Alice's asset. Charlie sets a value (t seconds) in the time lock [16], if Bob does not verify the cross-chain transaction or Bob does not transfer his asset within t seconds, or the transaction is suspended, the transaction will be terminated, and Alice's asset will be returned.

Step 4 Charlie receipts Alice's asset in the list, then Charlie initiates the QRS for the list, and the relay chain systematically allocates a validating node David and the leader node Emily for Charlie. Bob checks the transaction list and verifies the signature by his private key and all ring members' public key. After the verification succeeds, Bob transfers assets to Charlie and records them in the list.

Step 5 Charlie receives Bob's asset through an escrow account and places it in the pool of funds, and performs a time lock on it. Charlie exchanges the assets of Alice and Bob within the time lock. Upon receipt of Alice and Bob's return statement, Charlie generates a local transaction. The local transaction contains the transaction list and the verification proof of QRS. Charlie publishes the proof and submits the transaction to Emily.

Step 6 Alice and David conduct an audit. If the transaction records are valid, Emily validates the transaction and packages it into a new block in the relay chain. After the new block has been included in the relay chain by Emily, Charlie notifies Alice and Bob the cross-chain transaction is completed.

Charlie, an ordinary node, sends the transaction with the list to David, a validating node, for verification, if the verification succeeds, the verified transaction with the signature verification proof will be sent to Emily, the leader node, for validation.

Emily is also a ring member of the QRS, so that she can re-verify the signature by the signature verification proof. After validation, the transaction will be packaged in a new block; otherwise, it will be rejected. By the PoA mechanism in QCC, the leader node will strictly sort transactions in the transaction queue by timestamp and validate them individually. Invalid transactions will be rejected. Furthermore, even if a double-spending transaction is packaged in the new block by fault, the voting implemented by all validating nodes will vote down the faulty block. Thus, double spending is avoided.

Once the cross-chain transaction is included in the relay chain ledger, it becomes an untampered record maintained by all validating nodes in the relay chain, and no one can bear the computational burden and resource consumption required to tamper with the record.

2.2 Addressing the core challenges of cross-chain systems

Conventional cross-chain relays face three critical gaps: centralized trust dependencies, consensus vulnerabilities, and quantum threats. While classical post-quantum cryptography (e.g., lattice-based schemes) can mitigate the third threat, they often exacerbate the first two by increasing computational complexity and reliance on algorithmic assumptions. Our QCC model necessitates primitives that provide:

Decentralized Trust: Security should not depend on a single trusted authority.

Algorithmic Agility & Scalability: The framework must efficiently handle a growing number of heterogeneous chains and transactions.

Information-Theoretic Security Where Possible: Leveraging quantum physical principles can provide security guarantees beyond computational complexity.

2.3 Justification for the Two-Way Identity authentication (TIA) protocol

Tailored for Relay Trust Issues: A fundamental vulnerability in relay chains is the potential for malicious nodes to impersonate legitimate relays. TIA directly addresses this by enforcing mutual, information-theoretically secure authentication between the user (e.g., Alice) and the relay node (e.g., Charlie) in a single execution. This is more efficient and secure than executing two separate one-way authentications.

Information-Theoretic Security via Entanglement: TIA's security is rooted in the quantum correlations of GHZ states. As analyzed in Sect. 5.1, the probability of an adversary successfully forging an authentication session is bounded by $\eta = 1/8\hat{}n$, which becomes negligible for large n. This is superior to methods like Quantum Key Distribution (QKD), which only secures key exchange but does not inherently provide entity authentication. TIA uses QKD and One-Time Pad (OTP) as secure channels withinits workflow, but its core trust mechanism is the GHZ-state measurement.

Comparison with Alternatives: Other quantum signature-based authentication schemes often require a trusted third party for arbitration [23–29], which contradicts the decentralized ethos of blockchain. Lattice-based dynamic group signatures [19], while post-quantum secure, incur significant computational overhead and do not offer the same level of information-theoretic security for the initial handshake. TIA provides a more foundational level of trust for establishing node legitimacy.

2.4 Justification for the Quantum Ring Signature (QRS) scheme

Inherent Key-Loss Security: A critical, often overlooked risk in cross-chain systems is the long-term threat of key leakage through attacks or accidents. A paramount design goal was to ensure that a compromised key cannot be used to forge a valid signature. QRS achieves this through its dependence on locally generated, one-time quantum parameters (e.g., $|g(r)\rangle$). As proven in Sect. 5.2, even with a stolen classical key, an adversary cannot generate the correct quantum parameters to create a verifiable signature. This property is not a feature of standard digital signatures (even post-quantum ones) or most quantum signature schemes.

Built-in Decentralized Auditability: Unlike traditional or many quantum signatures that culminate in a single verification point, QRS is designed for distributed verification. Multiple entities (the initiator Alice and the validating node David) can independently and efficiently audit the signature's validity using the published proof. This decentralizes the trust in the relay chain itself and enables cross-chain consensus transmission, as the audit serves as a consensus checkpoint between the application chain and the relay chain. This is a unique feature tailored for blockchain interoperability.

Efficiency and Scalability for Multi-Party Scenarios: The ring signature structure is inherently suitable for the multi-party nature of a cross-chain transaction (involving users and different relay nodes). As demonstrated in Sect. 6.3 (and illustrated in Fig. 3), the computational overhead of QRS scales linearly with the number of ring members, and its latency remains stable. This makes it more practical for complex transactions compared to other quantum multi-signature schemes that may require more complex state preparations or verifications.

3 Access control in QCC

Usually, a unique user needs to register multiple identities in diverse blockchain systems. Furthermore, due to the business requirements across different scenarios, users' accounts (identities) in multiple blockchain systems are not related to each other. Moreover, cross-chain identity authentication management is the cornerstone for trustworthy interaction across blockchains. Therefore, this section proposes a global identity that can be utilized for heterogeneous blockchains, and a identity-based TIA protocol. The scheme uses an authorization model to transfer user access management to the application chain manager node to decentralize the pressure of the network nodes accessing the QCC system.

3.1 Identity registration in QCC

3.1.1 Application chain identification

To publish a cross-chain transaction, an application chain, i.e., chain A, must register in the relay chain to be authorized as a legal user chain beforehand. Chain A can only participate in cross-chain transactions once registered in the relay chain. The relay chain is an identity authority center that generates a unique identity denoted as Chain_ID for each application chain.

Digital Identity (ID) is a verifiable decentralized digital identity. In the QCC model, the ID is the unique user identification in the cross-chain network. QCC issues a global identity to the application chain and authorizes the assignment of the user identity to the application chain manager node. The user' ID includes the digital identity of both the application chain and the specific user.

The global identity of an application chain in the cross-chain network is the digital identity of a blockchain (chain_ID), the application chain that obtains the digital identity will have permission to issue a global identity for a user. The user identity ID consists of its application chain identity chain_ID and account identity account_ID. The account_ID is the user's unique identifier on each chain, which the application chain manager node assigns. A user is audited and authenticated by the internal manager node of the application chain.

A user's ID is a unique identifier, and the digital identity of all the application chains and users in the cross-chain network are stored in the relay chain. Legally registered users in the cross-chain network can initiate cross-chain transactions and acquire the resource.

3.1.2 Application chain registration

If chain A requires access to the cross-chain network for exchanging cross-chain data with other application chains, it must register its identity in the cross-chain network in advance. Chain A initiates a registration request by sending its blockchain information to the relay chain, such as the permission type, the consensus mechanism, and other information. After verification, the relay chain issues chain A with the identity chain_ID and a relay server session key within a time range, the session key is updated periodically by a routing protocol, and the session keys of each application chain are independent of each other. After chain A accepts chain_ID and session key, the registration in the relay chain will be initiated, and after that, chain A is a legal user chain in the cross-chain network.

3.2 Two-way identity authentication

An application chain user can issue a cross-chain transaction with other legally registered applications after being registered in the relay chain. The TIA will be initiated before processing a cross-chain transaction.

In cross-chain transactions through a relay chain, the security and reliability of the relay chain are the most important part to ensure the security of the transactions. Since the relay chain is the middleman responsible for information exchange and asset transferring, if they are disguised by malicious nodes, asset losses or data leakage will inevitably occur. For this issue, the TIA implements two-way authentication between the initiator and the relay node (middleman). If the initiator and the relay node pass the authentication, the cross-chain transaction will be processed and forwarded. The TIA avoids unauthorized users and malicious relay nodes, and it improves asset security on the application chain.

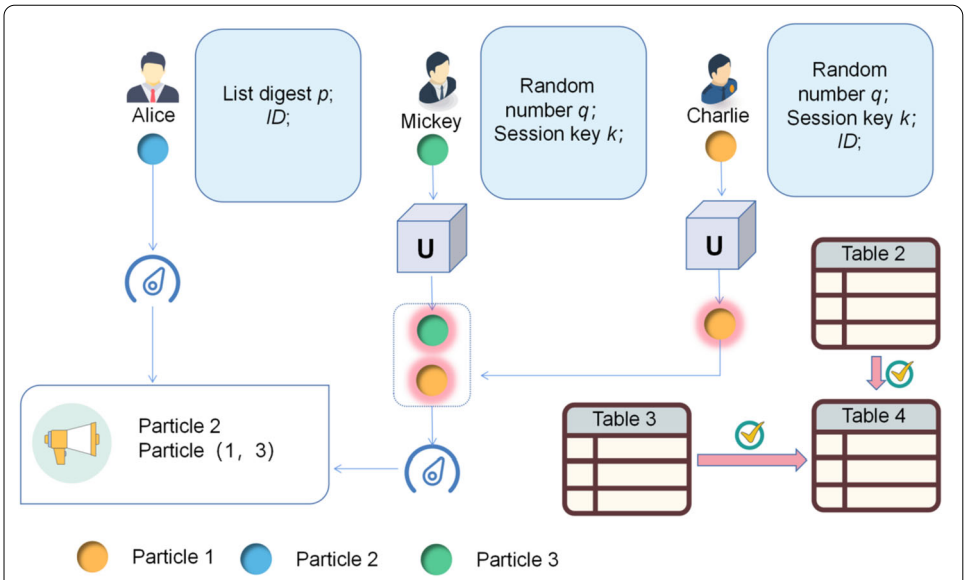

Figure 2 Model process of TIA

Suppose a cross-chain transaction with initiator Alice in chain A and the destination node Bob in chain B is sent to the relay chain, identity authentication is performed at first. In TIA, the manager node in Chain A–Mickey and Charlie in the relay chain participate in the authentication. The TIA protocol consists of two phases: initialization and authentication, the process of the TIA protocol is shown in Fig. 2.

In this section, a two-way identity authentication protocol for access control is proposed based on GHZ particles. The protocol needs to be executed only once to accomplish the authentication of both sides, instead of executing a one-way authentication protocol twice back and forth, which improves the efficiency of cross-chain transactions. Quantum key distribution (QKD) and one-time pad (OTP) [30–32] are combined in the protocol for secure data transmission.

3.2.1 Initialization

For any strings $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$, we define $x \| y = (x_1 \| y_1, x_2 \| y_2, \ldots, x_n \| y_n)$ and $x \oplus y = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$, where the symbol "$\|$" denotes the concatenation of strings, and the symbol "$\oplus$" denotes an XOR operation.

Bell state is a special two-particle entangled state. They are expressed as follows, respectively.

$$\begin{aligned} \left|\phi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \left|\phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \\ \left|\psi^+\right\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \end{aligned} \tag{1}$$

Let's say that Alice's identification is $ID_A \in (0,1)^n$, it is kept in Charlie's registry. An n-bit session key k with Charlie is kept by the manager node Mickey, $p_i \in (0,1)$, $i = 1, 2, \ldots, n$ stands for the digest of the list.

Table 1 The relationship of $p_i||ID_{A(i)}$ and operation, and $q_i||k_i$ and operation on particle 1

$p_i\|\|ID_{A(i)}$ $q_i\|\|k_i$	00	01	10	11
unitary operators	I	X	Y	Z

Table 2 The relationship between $q_i||ID_{A(i)}$ and B

$q_i\|\|ID_{A(i)}$	01/10	00/11
$B_{(i)}$	$\left\|\psi^-\right\rangle$ or $\left\|\phi^-\right\rangle$	$\left\|\psi^+\right\rangle$ or $\left\|\phi^+\right\rangle$

I-step1: By performing the quantum key distribution (QKD) protocol [33], Alice initiates a request for a cross-chain transaction and sends p_i to Charlie, p_i is only visible to Charlie due to protocol security.

I-step2: Upon receipt of the request, Charlie looks up Alice's registration $ID_A \in (0,1)^n$ based on her source address, and Charlie sends an n-bit key e to Mickey by QKD.

I-step3: Charlie generates a secret random number $q \in (0,1)^n$, calculates $e' = e \oplus q$, and sends Mickey e'.

I-step4: Mickey informs Alice to generates n GHZ states, which are indicated as

$$|\xi\rangle_{123} = \frac{1}{2}\left(|000\rangle + |110\rangle + |011\rangle + |101\rangle\right), \tag{2}$$

Alice sends particle 1 to Charlie, sends particle 3 to Mickey, and keeps particle 2 for herself.

3.2.2 Authentication

A-step1: Mickey computes and keeps the random number $q = e' \oplus e$ secretly after receiving e'.

A-step2: According to $p_i||ID_{A(i)}$, Charlie performs I, X, Y and Z unitary operators on particle 1 if $p_i||ID_{A(i)}$ are 00, 01, 10, 11, respectively. The details are shown in Table 1 as follows. Similarly, according to $q_i||k_i$, Mickey performs I, X, Y and Z unitary operators on particle 3 if $q_i||k_i$ are 00, 01, 10 and 11, respectively. The details are illustrated in Table 1 as follows. For example, if the $p_i||ID_{A(i)} = 01$, $q_i||k_i = 10$, it can get $\langle 0_2|\xi\rangle_{13} = \frac{1}{2}(|00\rangle - |11\rangle)$, $\langle 1_2|\xi\rangle_{13} = \frac{1}{2}(|10\rangle - |01\rangle)$.

A-step3: Alice measures particle 2, by $\{|1\rangle, |0\rangle\}$, and if $|\xi\rangle_2 = |1\rangle$, Alice restores $R = 1$, and vice versa. at the same time, particle 1 and 3 will collapse to the corresponding state.

A-step4: Charlie sends Mickey the particle 1 $\left|\xi'\right\rangle_1$, and computes $C_i = p_i||ID_i \oplus q_i||k_i$, $C_{(i)} \in (00, 01, 10, 11)^n$.

A-step5: After receiving the particle 1, Mickey performs Bell state joint measurement on particles (1,3). Moreover, the outcomes are denoted as $B_i \in \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$.

A-step6: Mickey determines whether the following relationships of the bits $q_i||ID_{A(i)}$ and B are valid. Table 2 provides the detail. Charlie will carry out A-step7 if it is satisfied. The identity is invalid otherwise.

A-step7: Charlie checks whether the following relationships of the bits C, R and B are satisfied.

The detail is shown in Table 3. If it is satisfied, Charlie passes the identity authentication, Alice sends p_i to Mickey, and he will perform A-step8. Otherwise, the transaction is terminated.

Table 3 The relationship between C, R and B

$R_{(i)}$	$C_{(i)}$			
	00	01	10	11
0	$B_{(i)} = \left\|\phi^+\right\rangle$	$B_{(i)} = \left\|\psi^+\right\rangle$ or $\left\|\psi^-\right\rangle$	$B_{(i)} = \left\|\psi^-\right\rangle$ or $\left\|\phi^-\right\rangle$	$B_{(i)} = \left\|\phi^-\right\rangle$
1	$B_{(i)} = \left\|\psi^-\right\rangle$	$B_{(i)} = \left\|\phi^+\right\rangle$	$B_{(i)} = \left\|\phi^-\right\rangle$	$B_{(i)} = \left\|\psi^-\right\rangle$

Table 4 The relationship between R and $k_i||p_i$

$k_i\|\|p_i$	00/10	01/11
R	0	1

A-step8: Mickey determines whether the following relationships of the bits R and $k_i||p_i$ are met. Table 4 contains the detail. If satisfied, Alice passes the identity authentication, Charlie returns the authentication result to Alice. The cross-chain transaction will be rejected if Alice fails in the identity authentication.

After Alice passes the identity authentication, Charlie checks Bob's ID in the relay chain ledger to confirm his identity. Charlie informs Alice that the cross-chain transaction request is permitted and forwarded if Bob is a legitimate user registered in the relay chain,. The transaction execution phase begins with the transaction request.

4 Quantum ring signature

To achieve post-quantum security, scholars have done significant works [23–29, 34–36]. In contrast, the adoption of a signature in a relay chain and how to enhance cross-chain transaction security and improve consensus transmission in heterogeneous blockchain is rarely investigated. The majority of quantum signatures cannot truly be applied to blockchain networks because the fully trusted centralization of most of them is against the decentralization of blockchain. In addition to the issues of efficiency and security, quantum's physical properties of measuring collapse are not compatible with the transaction verification of blockchain.

In a QCC transaction, after the QRS is generated, Bob must use his private key and the public key of the ring member for verification. The QRS includes five members: the initiator Alice, the receiver Bob, an ordinary node Charlie in the relay chain, a validating node David in the relay chain, and a leader node Emily in the relay chain. The leader node, validating node, and the ordinary node identity are disclosed in the relay chain under the POA consensus mechanism. The identity is disclosed during signature verification and forwarding to facilitate the audit and recording of transactions. The QRS in the transaction stage is shown in Algorithm 1.

For clarity, the following description of the algorithm focuses solely on the operations at the network and data layers, excluding the consensus layer.

The operators in QRS are defined as follows:

$$\text{a) } X_\delta = e^{-i\delta\frac{X}{2}} = \cos\frac{\delta}{2}I - i\sin\frac{\delta}{2}X, \tag{3}$$

$$\text{b) } Y_\vartheta = e^{-i\vartheta\frac{Y}{2}} = \cos\frac{\vartheta}{2}I - i\sin\frac{\vartheta}{2}Y, \tag{4}$$

$$\text{c) Hadamard Gate } H = \frac{1}{\sqrt{2}}[(|0\rangle\langle 1|)\langle 0| + (|0\rangle - |1\rangle)\langle 1|], \tag{5}$$

Algorithm 1 The signature by Charlie in QCC

{
Input: m, ring member
Output: $r_a^j \in (0,1)$, $r_b^j \in (0,1)$, $r_c^j \in (0,1)$, $r_d^j \in (0,1)$, and $r_e^j \in (0,1)$, $j = 1,2,\ldots,q$.
Input: r_a^j, r_b^j, r_c^j, r_d^j, r_e^j
Output: $\{\left|g\left(r_a^j\right)\right|, \left|g\left(r_b^j\right)\right|, \left|g\left(r_c^j\right)\right|, \left|g\left(r_d^j\right)\right|, \left|g\left(r_e^j\right)\right|\}$
Charlie computes the signature
$W_j^C = \left(W_1^C, W_2^C, \ldots, W_q^C\right)$
publishes the signature inside the ring, and uploads the quantum parameter $\{\left|g\left(r_a^j\right)\right|, \left|g\left(r_b^j\right)\right|, \left|g\left(r_c^j\right)\right|, \left|g\left(r_d^j\right)\right|, \left|g\left(r_e^j\right)\right|\}$ *to the quantum register.*
Bob computes
$\overline{W}_j^C = W_j^C|0\rangle = \left(\overline{W}_1^C, \overline{W}_2^C, \ldots, \overline{W}_q^C\right)$
$\overline{W}_j^B = W_j^B|0\rangle = \left(\overline{W}_1^B, \overline{W}_2^B, \ldots, \overline{W}_q^B\right)$
verifies
If $(\overline{W}_j^C = \overline{W}_j^B)$
  return valid!
Else
  return verification failed!
}

The operation of the logic gate H is shown as follows:

$$H|0\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) = |+\rangle, \tag{6}$$

$$H|1\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle) = |-\rangle, \tag{7}$$

The following is a definition of the quantum one-way function (QOWF) [37]:

Definition 1 (QOWF) A function $f : k \to |f_k\rangle$, where $|f_k\rangle$ satisfies $\langle f_k | f_k'\rangle \le \delta < 1$ for $k \ne k'$. It has the following properties:

1) Easy to compute: The mapping $f : k \to |f_k\rangle$ is simple to compute using a quantum polynomial-time algorithm.
2) Hard to invert: Given $|f_k\rangle$, it is impossible to invert k by fundamental quantum information theory.

The single-qubit rotation operator [20, 30] is employed in QRS. Let the operator $R(\theta) = e^{\frac{-i\theta Y}{2}}$, $S(\delta) = e^{\frac{-i\delta X}{2}}$, where the $\theta = \frac{\pi}{2^{n_\theta - 1}}$, $\delta = \frac{\pi}{2^{n_\delta - 1}}$, and $n_\theta \in N$, $n_\delta \in N$ are security parameters.

In light of this, we develop two one-way functions (QOWF): $x \to |f(x)\rangle$, and $r \to |g(r)\rangle$. The formula can be expressed as

$$|f(x)\rangle = R(x\theta)|0\rangle, \tag{8}$$

$$|g(r)\rangle = S(r\delta)H^{m_j \oplus ID}|+\rangle, \tag{9}$$

Where the $x \in N$ is the private key for a member in the ring, and $r \in N$ is the security parameter. The inner product space in Eqs. (8)–(9) can represent the linear operator of the outer product.

We define that

$$G_j = (\left|f\left(x\right)\right\rangle, \left|g\left(r\right)\right\rangle), \tag{10}$$

$$T_j = (\left|f\left(x\right)\right\rangle, \left\langle g\left(r\right)\right|), \tag{11}$$

For example,

$$G_j^{AB} = \left(\left|f\left(a\right)\right\rangle, g\left(r_b\right)\right), \tag{12}$$

$$T_j^{A} = \left(\left|f\left(a\right)\right\rangle, g\left(r_a\right)\right). \tag{13}$$

According to the property of inner product space, it is clear that

$$\left\langle g\left(r\right)\right| T_j = \alpha G_j \left\langle g\left(r\right)\right|, \tag{14}$$

where the α is denoted as a constant coefficient.

Suppose that $m_j = (m_1, m_2, \ldots m_q) \in (0,1)^q$ is the digest of list to be signed. Charlie randomly chooses a parameter $c_j = (c_1, c_2, \ldots, c_q) \in (0,1)^q$ as his private key, and then Charlie calculates his public key

$$\left|f(c_j)\right\rangle = e^{\frac{-ic_j\theta Y}{2}}\left|0\right\rangle, \tag{15}$$

and publishes it. The public keys will be saved in the quantum register.

Similarly, Alice, Bob, David, and Emily select their private key $a_j \in (0,1)^q$, $b_j \in (0,1)^q$, $d_j \in (0,1)^q$, and $e_j \in (0,1)^q$, $j = 1, 2, \ldots, q$. Therefore, the corresponding public keys are calculated separately,

$$\left|f(a_j)\right\rangle = e^{\frac{-ia_j\theta Y}{2}}\left|0\right\rangle, \tag{16}$$

$$\left|f(b_j)\right\rangle = e^{\frac{-ib_j\theta Y}{2}}\left|0\right\rangle, \tag{17}$$

$$\left|f(d_j)\right\rangle = e^{\frac{-id_j\theta Y}{2}}\left|0\right\rangle, \tag{18}$$

$$\left|f(e_j)\right\rangle = e^{\frac{-ie_j\theta Y}{2}}\left|0\right\rangle. \tag{19}$$

and then they publish it in the ring.

(1) Signing phase

Let $ID_{\mathrm{A}}, ID_{\mathrm{B}}, ID_{\mathrm{C}}, ID_{\mathrm{D}}, ID_E \in (0,1)^q$ denote the identification information of Alice, Bob, Charlie, David and Emily.

S-step1: Charlie randomly selects parameters for herself, Alice, Bob, David and Emily, respectively. It is denoted as $r_c^j \in (0,1)$, $r_a^j \in (0,1)$, $r_b^j \in (0,1)$, $r_d^j \in (0,1)$ and $r_e^j \in (0,1)$, $j = 1, 2, \ldots, q$. Then Charlie will compute quantum parameter $\left\langle g(r)\right|$ on the message m. Accordingly, the quantum parameter $\left\{\left\langle g(r_a^j)\right|, \left\langle g(r_b^j)\right|, \left\langle g(r_c^j)\right|, \left\langle g(r_d^j)\right|, \left\langle g(r_e^j)\right|\right\}$ is uploaded

to the quantum register, note that the parameter uploaded by a member is stored in a directory named by his/her ID in the register.

The quantum parameters are one-time-dense, that is, new quantum parameters must be generated every time according to transaction message and local parameters when the transaction is carried out, and the classical parameters of the quantum parameters that have participated in the verification will be stored in the ledger as a proof.

$$\left|g\left(r_a^j\right)\right\rangle = e^{\frac{-ir_a^j\delta X}{2}} H^{m_j\oplus ID_A}\left|+\right\rangle, \tag{20}$$

$$\left|g\left(r_b^j\right)\right\rangle = e^{\frac{-ir_b^j\delta X}{2}} H^{m_j\oplus ID_B}\left|+\right\rangle, \tag{21}$$

$$\left|g\left(r_c^j\right)\right\rangle = e^{\frac{-ir_c^j\delta X}{2}} H^{m_j\oplus ID_C}\left|+\right\rangle, \tag{22}$$

$$\left|g\left(r_d^j\right)\right\rangle = e^{\frac{-ir_d^j\delta X}{2}} H^{m_j\oplus ID_D}\left|+\right\rangle, \tag{23}$$

$$\left|g\left(r_e^j\right)\right\rangle = e^{\frac{-ir_e^j\delta X}{2}} H^{m_j\oplus ID_E}\left|+\right\rangle, \tag{24}$$

S-step2: According to Eqs. (10)–(14) and (16)–(24), Charlie computes

$$\begin{aligned} W_j^C &= R(\theta_c)\left\langle g\left(r_c^j\right)\right| T_j^A T_j^B T_j^D T_j^E \\ &= R(\theta_c) G_j^{CA} G_j^{AB} G_j^{BD} G_j^{DE}\left\langle g\left(r_e^j\right)\right| \\ &= e^{\frac{-ic_i\theta Y}{2}} \cdot \left\langle g\left(r_c^j\right)\right| \left|f\left(a_j\right)\right\rangle \left\langle g\left(r_a^j\right)\right| \left|f\left(b_j\right)\right\rangle \left\langle g\left(r_b^j\right)\right|, \\ &\left|f\left(d_j\right)\right\rangle \left\langle g\left(r_d^j\right)\right| \left|f\left(e_j\right)\right\rangle \left\langle g\left(r_e^j\right)\right| \left(j = 1, 2, \ldots, q\right) \end{aligned} \tag{25}$$

Charlie publishes the signature $W_j^C = \left(W_1^C, W_2^C, \ldots, W_q^C\right)$ inside the ring.

(2) Verifying phase

The ordinary node Bob is a member of the ring, and he will verify this signature.

V-step1: After downloading a copy of the public key from the quantum register, Bob computes

$$\overline{W}_j^C = W_j^C\left|0\right\rangle = \left(\overline{W}_1^C, \overline{W}_2^C, \ldots, \overline{W}_q^C\right), \tag{26}$$

$$\begin{aligned} \overline{W}_j^B &= W_j^B\left|0\right\rangle = R(\theta_b)\left\langle g\left(r_b^j\right)\right| T_j^A T_j^C T_j^D T_j^E \\ &= R(\theta_b) G_j^{BA} G_j^{AC} G_j^{CD} G_j^{DE}\left\langle g\left(r_e^j\right)\right| \left|0\right\rangle \left(j = 1, 2, \ldots, q\right) \end{aligned}, \tag{27}$$

V-step2: Bob checks whether $\overline{W}_j^C$ and $\overline{W}_j^B$ are equal or not. If they are equal, Bob checks $\{r_a, r_b, r_c, r_d, r_e\}$ publishes it. $\{r_a, r_b, r_c, r_d, r_e\}$ and $\overline{W}_j^C = \overline{W}_j^B$ will be stored in the classical register as proof for validation.

In addition, quantum registers release quantum states $\left\{\left\langle g(r_a^j)\right|, \left\langle g(r_b^j)\right|, \left\langle g(r_c^j)\right|, \left\langle g(r_d^j)\right|, \left\langle g(r_e^j)\right|\right\}$; Emily packages the transaction into a new block to record it in the relay chain.

5 Security analysis

5.1 Algorithm security

5.1.1 Security analysis of TIA

Identity authentication protects cross-chain access, and it's a prerequisite for secure transactions. It is a more secure access control policy for end-to-end cross-chain networks to confirm each other's identities.

In cross-chain transactions, Alice must not imitate manager for identity authentication and access management; otherwise, malicious users may conduct illegal transactions; moreover, manager must not disguise relay nodes for identity authentication of legitimate users; otherwise, malicious manager may obtain assets illegally.

First, Alice can't fake the operation of manager Mickey, because q_i and k_i is secretly saved by Mickey according to A-step3, due to the unconditionally security of QKD and OTP, Alice can not break them. Then, Mickey can't fake the operation of Charlie, because p_i is only visible to Charlie due to protocol security according to A-step2. Therefore, both internal and external nodes of the cross-chain network, the only way for the attacker to obtain the corresponding quantum operation is to obtain the $p_i||ID_i$ and $q_i||k_i$, which are control parameters for particle 1 and 3.

Assume Eve, the attacker, wants to forge the signature. He needs to use the correct quantum gate transformation to choose the correct operation based on $p_i||ID_i$ and $q_i||k_i$. Where p_i is invisible to Eve, for each particle he has a 1/4 chance of guessing, then the probability of the operation being valid is $\eta = 1/4^{2n}$. In addition, since the QKD and OTP is unconditionally secure, q_i cannot be intercepted, and p_i does not need to be transmitted through the channel, so the conversion operation of each GHZ particle has a 1/8 probability of guessing, so the probability of the authentication being valid is $\eta = 1/8^n$. It can be observed that when n becomes large enough, the probability η is close to 0. As a result, the scheme cannot be forged and can avoid forgery. And once two-way authentication is passed, the relay node cannot maliciously reject cross-chain requests. Last but not the least, two-way authentication can improve the reliability of the relay chain.

5.1.2 Security analysis of QRS

Correctness: $\{W_j\}$ is the quantum signature encrypted based on an asymmetric key. Given the encrypted message's quantum parameters, each ring member can verify using their private key and the other member's public key. If the signature is genuine, the equality of the calculated results can be confirmed. The proof will be presented as follows.

$$\begin{aligned}
\overline{W}_j^C &= W_j^C|0\rangle = R(\theta_c)\left\langle g\left(r_c^j\right)\right| T_j^A T_j^B T_j^D T_j^E|0\rangle \\
&= \left(e^{\frac{-i(r_a+r_b+r_c+r_d+r_e)\delta X}{2}} H^{ID_a\oplus ID_b\oplus ID_c\oplus ID_e}\left|+\right\rangle, e^{\frac{-i(a+b+c+d+e)\theta Y}{2}}|0\rangle\right), \\
&= \left(\left|f\left(a_j+b_j+c_j+d_j+e_j\right)\right\rangle, \left|g\left(r_a^j+r_b^j+r_c^j+r_d^j+r_e^j\right)\right\rangle\right)
\end{aligned} \tag{28}$$

And we can get

$$\begin{aligned}
\overline{W}_j^B &= W_j^B|0\rangle = R(\theta_b)\left\langle g\left(r_b^j\right)\right| T_j^A T_j^C T_j^D T_j^E|0\rangle \\
&= \left(e^{\frac{-i(r_a+r_b+r_c+r_d+r_e)\delta X}{2}} H^{ID_a\oplus ID_b\oplus ID_c\oplus ID_e}\left|+\right\rangle, e^{\frac{-i(a+b+c+d+e)\theta Y}{2}}|0\rangle\right), \\
&= \left(\left|f\left(a_j+b_j+c_j+d_j+e_j\right)\right\rangle, \left|g\left(r_a^j+r_b^j+r_c^j+r_d^j+r_e^j\right)\right\rangle\right)
\end{aligned} \tag{29}$$

It is clear that $\overline{W}_j^C = \overline{W}_j^B$. In the same way, we can calculate $\overline{W}_j^A$, $\overline{W}_j^D$ and $\overline{W}_j^E$. The following formula holds

$$\overline{W}_j^A = \overline{W}_j^B = \overline{W}_j^C = \overline{W}_j^D = \overline{W}_j^E, \tag{30}$$

Since $\overline{W}_j^C = \overline{W}_j^B$ is a classical value, we only need to compare the values once to determine whether they are equal. The signature is accepted, provided that they are equal.

Information-theoretical security: In QRS, according to Eqs. (8)–(9) and (16)–(24), it can be seen that the private key is secretly saved, while the corresponding public key is generated by one-way function calculation. The one-way function's characteristics make it simple to calculate the private key from the public key, but not the other way around. Private keys, as a result, are safe and secret. The following shows that the parameters cannot be computed from the quantum state, Information-theoretic security analysis.

Secure cryptosystems are ciphertext indistinguishable under selective plaintext attack (IND-CPA) [38, 39]. A secure quantum public key cryptosystem has the indistinguishable property of ciphertext under quantum [40].

Theorem 1 *For all plaintexts x and y, let the density operators of cipher states E(x) and E(y) be ρ_x and ρ_y, respectively. For every positive polynomial $p(\cdot)$ and every sufficiently large n, there is hold*

$$D(\rho_x, \rho_y) < 1/p(n).$$

Theorem 2 *The QRS has the information-theoretical security.*

Proof In QRS, let $|g(r)|$ and $|g(r^*)|$ be the ciphertexts of different plaintexts m and m^*, respectively. The density operators of $\rho_{g(r),m}$ and $\rho_{g(r^*),m^*}$ should take all the possible values of m and ID. We can get

$$\begin{aligned}
\rho_{g(r),m} &= \frac{1}{2^{2q}} \otimes_{i=1}^{q} \sum_{m,ID} |g(r)\rangle\langle g(r)| \\
&= \frac{1}{2^{2q}} \otimes_{i=1}^{q} \sum_{m,ID} \left(e^{\frac{-i\delta X}{2}} H^{ID\oplus m} |+\rangle\langle+| H^{ID\oplus m} e^{\frac{-i\delta X}{2}} \right), \\
&= \otimes_{i=1}^{q} \rho_i
\end{aligned} \tag{31}$$

where $\rho_i \in \left\{ \begin{bmatrix} 1/4 & 1/4 \\ 1/4 & 3/4 \end{bmatrix} \right\}$.

Similarly, the density operator of $\rho_{g(r^*),m^*}$ can be computed as follow

$$\begin{aligned}
\rho_{g(r^*),m'^*} &= \frac{1}{2^{2q}} \otimes_{i=1}^{q} \sum_{m^*,ID} |g(r^*)\rangle\langle g(r^*)| \\
&= \frac{1}{2^{2q}} \otimes_{i=1}^{q} \sum_{m,ID} \left(e^{\frac{-i\delta X}{2}} H^{ID\oplus m^*} |+\rangle\langle+| H^{ID\oplus m^*} e^{\frac{-i\delta X}{2}} \right), \\
&= \otimes_{i=1}^{q} \rho_i^*
\end{aligned} \tag{32}$$

where $\rho_i^* \in \left\{ \begin{bmatrix} 1/4 & 1/4 \\ 1/4 & 3/4 \end{bmatrix} \right\}$. It is worth noting that

$$D(\rho_i, \rho_i^*) \leq \frac{\sqrt{2}}{2}. \tag{33}$$

It follows that

$$D(\rho_{g(r),m}, \rho_{g(r^*),m^*}) \leq (\frac{\sqrt{2}}{2})^n, \tag{34}$$

When the $n \to \infty$, it's easy to compute that

$$\lim_{n\to\infty} (\frac{\sqrt{2}}{2})^n = 0. \tag{35}$$

Therefore, the result of Theorem 2 means that no distinguishing algorithm D can distinguish the signatures $\{W_j\}$ and $\{W_j^*\}$ efficiently. This means that no efficient distinguishing algorithm D can break the signer's key, $g(r)$ and $g(r^*)$ are ciphertext indistinguishable under selective plaintext attack (IND-CPA). □

Theorem 3 *If an adversary Eve performs some unitary operator $U = \otimes_{i=1}^q U_i$ on the signature $\{W_j\}$, the signature's density operator will not have any change. For each message-signature pair (m, W_j), after the unitary operator attack $U = \otimes_{i=1}^q U_i$ on W_j, the density operator of the state of the disturbed quantum signature W_j is always ρ_i.*

Proof If an adversary Eve applies some unitary operator $U = \otimes_{i=1}^q U_i$ to W_j, the density operator of W_j can be computed as follows

$$\rho_i = \frac{1}{2} U_i \sum_{m,ID} \left(e^{\frac{-i\delta X}{2}} H^{ID\oplus m} \left| + \right\rangle\left\langle + \right| H^{ID\oplus m} e^{\frac{-i\delta X}{2}} \right) U_i^+ = \begin{bmatrix} 1/4 & 1/4 \\ 1/4 & 3/4 \end{bmatrix}. \tag{36}$$

As a result, the signature density operator will remain unchanged in case of a unitary operator attack.

Unforgeability and non-repudiation: In QCC model, after the ring members secretly generate the private key, they use it to calculate the quantum state of the public key and publish it in the ring. As a result, QRS can withstand denial and forgery attacks. When a cross-chain transaction is initiated, two application chain nodes and three relay chain nodes become ring members. In the following, the analysis will be provided.

Suppose through the consensus mechanism, Emily becomes the new ordinary node, Eve wants to impersonates Emily to sign message m'. In fact, during the relay chain transaction, other nodes not involved in the ring can't download the key in the temporary register, and calculate the correct quantum parameters from the local parameters. Here, we assume that Eve is a powerful attacker with quantum computing capabilities. Eve generates the secret parameter r' by himself and computes the quantum parameters.

$$\left| g\left(r_a'^j\right) \right\rangle = e^{\frac{-ir_a'^j \delta X}{2}} H^{m'^j \oplus ID_A} \left| + \right\rangle, \tag{37}$$

$$\left| g\left(r_b'^j\right) \right\rangle = e^{\frac{-ir_b'^j \delta X}{2}} H^{m'^j \oplus ID_B} \left| + \right\rangle, \tag{38}$$

$$\left|g\left(r_c'^j\right)\right\rangle = e^{\frac{-ir_c'^j\delta X}{2}} H^{m'_j \oplus ID_C} \left| + \right\rangle, \tag{39}$$

$$\left|g\left(r_d'^j\right)\right\rangle = e^{\frac{-ir_d'^j\delta X}{2}} H^{m'_j \oplus ID_D} \left| + \right\rangle, \tag{40}$$

$$\left|g\left(r_e'^j\right)\right\rangle = e^{\frac{-ir_e'^j\delta X}{2}} H^{m'_j \oplus ID_E} \left| + \right\rangle. \tag{41}$$

Because of QOWF security [29], and e is the key stored locally by the node, Eve has to guess a e' to forge the signature, and the signature $W_j'^E$ is expressed as

$$\begin{aligned} W_j'^E &= R(\theta_{e'}) \left\langle g\left(r_e'^j\right)\right| T_j^A T_j^B T_j^C T_j^D \\ &= R(\theta_{e'}) G_j^{E'A} G_j^{AB} G_j^{BC} G_j^{CD} \left\langle g\left(r_d'^j\right)\right| \\ &= e^{\frac{-ie'_j\theta Y}{2}} \cdot \left\langle g\left(r_e'^j\right)\right| \left|f\left(a_j\right)\right\rangle \left\langle g\left(r_a'^j\right)\right| \left|f\left(b_j\right)\right\rangle \left\langle g\left(r_b'^j\right)\right|, \\ &\left|f\left(c_j\right)\right\rangle \left\langle g\left(r_c'^j\right)\right| \left|f\left(d_j\right)\right\rangle \left\langle g\left(r_d'^j\right)\right| \left(j = 1, 2, \ldots, q\right) \end{aligned} \tag{42}$$

Note that the $e_j \in (0,1)^q$, the probability of Eve guessing is $1/2^q$, as the length of the key increases, the probability of $e' = e$ is infinitely close to 0, where $e = (e_1, e_2, \ldots, e^q) \in N^+$. There must be $\overline{W}_j'^E \neq \overline{W}_j^B$. The signature $\overline{W}_j'^E$ and $\overline{W}_j'^B$ is expressed as

$$\overline{W}_j'^E = W_j'^E|0\rangle = \left(\overline{W}_1'^E, \overline{W}_2'^E, \ldots, \overline{W}_q'^E\right), \tag{43}$$

$$\overline{W}_j'^B = W_j'^B|0\rangle = \left(\overline{W}_1'^B, \overline{W}_2'^B, \ldots, \overline{W}_q'^B\right). \tag{44}$$

Similarly, other members of the ring cannot accurately guess Emily's local secret private key, so they can only use the local private key and the public key of other members to sign. However, after generating the signature, Emily cannot claim that it is signed by other members. The proof is shown in the "5.2.3 *Key-loss security*" section below.

Others cannot obtain the inner ring member's private key. Only the personal private key, other's public keys, and quantum parameters can be used to generate a legitimate signature as long as it is a legitimate ring member. Therefore, the QRS is unforgeable and undeniable, once the ring signature is generated and verified, the ring member cannot deny the validity of the signature. □

5.2 Mechanism security

A quantum cross-chain model (QCC) is proposed for cross-chain trading. Due to the utilization of quantum cryptography like TIA and QRS in QCC with the PoA consensus mechanism, it is secure against quantum computing attacks and it is also efficient and scalable.

5.2.1 Secure cross-chain access

The QCC model uses the relay chain as an identity authority, achieving a global identity registration and authentication for heterogeneous application chain users. The global cross-chain identity entry solution facilitates and secures cross-chain transactions between application chains. Therein, the adopted TIA protocol uses the physical properties of quantum particles to perform the two-way identity authentication and restrict the participation of malicious nodes.

5.2.2 Cross-chain consensus transmission via audit

In general, cross-chain transaction security and asset security depend on the self-control ability of the relay chain, i.e., whether the relay nodes (intermediaries) are honest can only be supervised by the relay chain itself, and asset security can only be confirmed by post-facto review, and the risk of asset loss is greatly increased by the lagging processing of this mechanism in the event of mischief. However, in QCC, the network layer's cryptographic algorithm is invoked, i.e., QRS, to realize the distributed audit and validation synchronized with the transaction. Taking the transaction in the paper as an example, Alice and David enjoy equal audit rights, which means the decentralization of transaction credibility in the cross-chain mechanism, and the precautionary measures of real-time supervision and audit are achieved at the same time. For the rest, the QRS reduces the dependence on QCC and makes them semi-trusted, and reducing the risk of man-in-middle maliciousness such as tamper, forging or denial. Therefore, the QCC model enhances transaction security and integrity.

In a typical relay chain scheme, validating a cross-chain transaction requires three internal transaction inclusions in three blockchain systems (two application chains and the relay chain), in which verification of transactions is implemented by three parties separately. Moreover, the time-consuming and inefficient implementation of transactions inclusion in the three blockchains is necessary to complete a cross-chain transaction. In contrast, in the cross-chain transaction of QCC with the adoption of QRS, the audit of the initiating node will quickly reach the tripartite consistency with the relay chain and the target chain after the verification of the target chain node is passed, so as to facilitate the completion of bookkeeping and prevent cross-chain transactions from causing blockchain network congestion and failures. Thus it reduces the relay node's evil risk and improves the cross-chain transaction's security.

The QRS can audit the signature according to signature proof, and Alice, David can initiate it without a trusted center. In this transaction, after David and Alice pass the audit, the relay leader node Emily is allowed to verify the transaction and ledger. As the initiator in the chain A, Alice's audit ensures the integrity of the transaction source information, the legitimacy of the transaction, and the cross-chain consensus transmission between the chain A and the relay chain.

As a validating node, David downloads a copy of the signature proof $\{r_a, r_b, r_c, r_d, r_e\}$ and $\overline{W}_j^C = \overline{W}_j^B$ through the quantum register, and executes the following stage in Algorithm 2.

AV-step1: David computes quantum parameters according to Eqs. (20)–(24). Accordingly, he calculates

$$\begin{aligned} W_j^D &= R(\theta_d)\left\langle g\left(r_d^j\right)\right| T_j^A T_j^B T_j^C T_j^E \\ &= R(\theta_d) G_j^{DA} G_j^{AB} G_j^{BC} G_j^{CE} \left\langle g\left(r_e^j\right)\right| \left(j = 1, 2, \ldots, q\right) \end{aligned}, \tag{45}$$

$$\overline{W}_j^D = W_j^D|0\rangle = \left(\overline{W}_1^D, \overline{W}_2^D, \ldots, \overline{W}_q^D\right). \tag{46}$$

AV-step2: David compares $\overline{W}_j^C$ with $\overline{W}_j^D$. If they are equal, the signature is valid, and vice versa.

David's audit can avoid illegal transactions and accounting errors before the chain is recorded.

Algorithm 2 David's validation stage

{
Input: $m, r_a^j, r_b^j, r_c^j, r_d^j, r_e^j$
Output: $\{\left|g\left(r_a^j\right)\right\rangle, \left|g\left(r_b^j\right)\right\rangle, \left|g\left(r_c^j\right)\right\rangle, \left|g\left(r_d^j\right)\right\rangle, \left|g\left(r_e^j\right)\right\rangle\}$
David computes
$\overline{W}_j^D = W_j^D|0\rangle = \left(\overline{W}_1^D, \overline{W}_2^D, \ldots, \overline{W}_q^D\right)$
If $(\overline{W}_j^C = \overline{W}_j^D)$
return valid!
Else
return verification failed!
}

Algorithm 3 Alice's validation stage

{
Input: $m, r_a^j, r_b^j, r_c^j, r_d^j, r_e^j$
Output: $\{\left|g\left(r_a^j\right)\right\rangle, \left|g\left(r_b^j\right)\right\rangle, \left|g\left(r_c^j\right)\right\rangle, \left|g\left(r_d^j\right)\right\rangle, \left|g\left(r_e^j\right)\right\rangle\}$
Alice computes
$\overline{W}_j^A = W_j^A|0\rangle = \left(\overline{W}_1^A, \overline{W}_2^A, \ldots, \overline{W}_q^A\right)$
If $(\overline{W}_j^C = \overline{W}_j^A)$
return valid!
Else
return verification failed!
}

As an initiator node in Chain A, Alice checks whether the relay node has been tampered by audit, if not, the chain A agrees with the relay chain for accounting and block generation, at the same time, reaches consensus transmission with the relay chain.

Similarly, Alice downloads a copy of the signature proof $\{r_a, r_b, r_c, r_d, r_e\}$ and $\overline{W}_j^C = \overline{W}_j^B$ through the quantum register, and executes the following stage in Algorithm 3.

Alice's audit can prevent Charlie's tampering behavior, ensuring the integrity of the information source, and Alice plays as a certain supervisory role.

5.2.3 Key-loss security

There is a potential risk of illegal transactions in a conventional relay chain due to key leakage. However, the algorithm's security do not totally rely on the assumption of key security, which will provide algorithm with protection from the underlying asset theft and privacy leakage caused by key theft or force majeure factors. The cross-chain transaction of QCC is further protected by the key-loss security, the transaction security in the relay network is strengthened by using the cryptographic mechanism.

In QRS, the stolen or leaked key cannot be used to issue legal ring signature, preventing the malicious node in QCC from using the legal key to carry out cross-chain transactions. If the adversary Eve possesses the key e by chance, Eve intercepts Emily's signature and signed the tampered message m'. Eve computes Eqs. (37)–(41) and uploads it, and he

computes the signature

$$\begin{aligned} W_j'^E &= R(\theta_e)\left\langle g\left(r_e^j\right)\right| T_j^A T_j^B T_j^C T_j^D \\ &= R(\theta_e) G_j^{EA} G_j^{AB} G_j^{BC} G_j^{CD} \left\langle g\left(r_d'^j\right)\right| \\ &= e^{\frac{-ie_j\theta Y}{2}} \cdot \left\langle g\left(r_e'^j\right)\right| \left|f\left(a_j\right)\right\rangle \left\langle g\left(r_a'^j\right)\right| \left|f\left(b_j\right)\right\rangle \left\langle g\left(r_b'^j\right)\right| \cdot \\ &\left|f\left(c_j\right)\right\rangle \left\langle g\left(r_c'^j\right)\right| \left|f\left(d_j\right)\right\rangle \left\langle g\left(r_d'^j\right)\right| \left(j = 1, 2, \ldots, q\right) \end{aligned} \tag{47}$$

In QRS, the signing node must secretly generate the quantum parameters using the classical parameters. Only the signing node can upload them, meaning no one can obtain the local classical parameters except the signing node. The malicious node can only forge another set of classical parameters to calculate the quantum parameters. Assuming that these fake quantum parameters in Eqs. (37)–(41) are uploaded to the register, Emily will find an unusual update to her own quantum parameters. Then she can initiate validation and calculate the quantum parameters generated by the local random warp $\left\{\left\langle g(r_a^j)\right|, \left\langle g(r_b^j)\right|, \left\langle g(r_c^j\right|, \left\langle g(r_d^j)\right|, \left\langle g(r_e^j)\right|\right\}$. Emily will find that the uploaded parameters are forged by comparing the quantum exchange test.

Similarly, if another ring member claims to be Emily signs a transaction with personal local private key and other members' public keys, Emily will detect the evil through local parameter calculation of QOWF [29]. Therefore, legitimate nodes will easily find that the parameters are inconsistent with those generated locally.

5.3 Formal verification via quantum hoare logic

To rigorously prove the composite security of the TIA protocol and QRS scheme (i.e., that TIA's secure authentication process does not weaken QRS's unforgeability, and their synergy can resist man-in-the-middle attacks), we employ the Quantum Hoare Logic (QHL) [41] framework proposed by Ying for formal verification. This logic uses Hermitian operators as quantum predicates to precisely describe entangled state evolution and knowledge preservation properties.

First, we abstract TIA and QRS as quantum program compositions. Let the total system Hilbert space be:

$$\mathcal{H}_{sys} = \mathcal{H}_{Alice} \otimes \mathcal{H}_{Charlie} \otimes \mathcal{H}_{Mickey} \otimes \mathcal{H}_{relay} \otimes \mathcal{H}_{aux}. \tag{48}$$

Where $\mathcal{H}_{relay}$ is the quantum register of the relay chain, and $\mathcal{H}_{aux}$ is the auxiliary space of adversary Eve.

5.3.1 Security invariants of TIA protocol

Define core quantum predicates for the TIA process, characterizing knowledge isolation during authentication:

$$\mathcal{P}_{TIA} \equiv \otimes_{i=1}^{n} \left(\frac{1}{2}I + \frac{1}{2}Z\right)_{C_i} \otimes \left(\frac{1}{2}I + \frac{1}{2}X\right)_{M_i} \otimes \left(\frac{1}{2}I + \frac{1}{2}Y\right)_{A_i}, \tag{49}$$

where subscripts C_i, M_i, A_i denote the i-th quantum bit of Charlie, Mickey, and Alice, respectively. This predicate encodes the binding relationship between classical parameters and quantum operations:

a. Only when $\boldsymbol{ID_A} \oplus \boldsymbol{p_i}$ is correct does Charlie's particle 1 collapse to the correct eigenstate in the X-basis.
b. Only when $\boldsymbol{k_i} \oplus \boldsymbol{q_i}$ is correct does Mickey's particle 3 collapse to the correct eigenstate in the Y-basis.

Key Lemma 1 *For any adversary auxiliary space* $\mathcal{H}_{\mathbf{Eve}}$*, after executing TIA, the following holds*:

$$\{\mathcal{P}_{\boldsymbol{TIA}} \otimes \boldsymbol{I_{Eve}}\}\boldsymbol{TIA\_Auth}\{\mathcal{P}'_{\boldsymbol{TIA}}\}, \tag{50}$$

where $\boldsymbol{P'_{TIA}}$ *ensures Parameter Confidentiality, Information entropy loss of* $\boldsymbol{p_i}, \boldsymbol{q_i}, \boldsymbol{k_i}$*, does not exceed* $\mathbf{2}^{-\boldsymbol{n}}$*, and Authentication Binding, After successful authentication, subspaces* $\mathcal{H}_{\mathbf{Alice}}$ *and* $\mathcal{H}_{\boldsymbol{Charlie}}$ *establish quantum correlation via GHZ states*; *any tampering with authentication results causes state fidelity* $\boldsymbol{F} < \mathbf{1} - \mathbf{2}^{-\boldsymbol{n}}$.

Proof Apply QHL rules to each step of TIA:

I-step1: Apply quantum parallel composition rule and BB84 security axiom, ensuring quantum inaccessibility of $\boldsymbol{p_i}$.

A-step2: Apply unitary transformation rule, $\{\boldsymbol{P}\}\boldsymbol{U}\{\boldsymbol{U}^{\dagger}\boldsymbol{P}\boldsymbol{U}\}$, where $\boldsymbol{U} = \otimes_{\boldsymbol{i}}\boldsymbol{U}_{\boldsymbol{C_i}}(\boldsymbol{p_i}\|\boldsymbol{ID}_{\boldsymbol{A(i)}}) \otimes \boldsymbol{U}_{\boldsymbol{M_i}}(\boldsymbol{k_i}\|\boldsymbol{q_i})$, ensuring one-to-one correspondence between operations and classical parameters.

A-step5: Apply measurement rule, where measurement result $\boldsymbol{B_i}$ is recorded as a classical ghost variable, satisfying deterministic relationships with quantum state collapse outcomes □

5.3.2 Unforgeability reduction of QRS

Define security predicates for QRS, characterizing signature integrity:

$$\mathcal{P}_{\boldsymbol{QRS}} \equiv \forall \boldsymbol{j} \in [\mathbf{1}, \boldsymbol{q}] : |\overline{\boldsymbol{W}}_{\boldsymbol{j}}^{\boldsymbol{C}}\rangle\langle\overline{\boldsymbol{W}}_{\boldsymbol{j}}^{\boldsymbol{C}}| = \otimes_{\boldsymbol{m}\in\{\boldsymbol{A},\boldsymbol{B},\boldsymbol{D},\boldsymbol{E}\}}\langle \boldsymbol{g}(\boldsymbol{r}_{\boldsymbol{m}}^{\boldsymbol{j}})|\boldsymbol{f}(\boldsymbol{x}_{\boldsymbol{m}}^{\boldsymbol{j}})\rangle \cdot \langle \boldsymbol{f}(\boldsymbol{x}_{\boldsymbol{m}}^{\boldsymbol{j}})|\boldsymbol{g}(\boldsymbol{r}_{\boldsymbol{m}}^{\boldsymbol{j}})\rangle. \tag{51}$$

This predicate asserts that the signature state $\overline{\boldsymbol{W}}_{\boldsymbol{j}}^{\boldsymbol{C}}$ is the tensor product of inner products of each member's quantum one-way function.

Key Lemma 2 *After successful TIA execution, if an adversary attempts to forge a signature, the success probability is constrained by*

$$\{\mathcal{P}_{\boldsymbol{TIA}} \wedge (\boldsymbol{ID_A}, \boldsymbol{ID_B} \in \boldsymbol{Ledger})\}\boldsymbol{QRS\_Sign}\{\mathcal{P}_{\boldsymbol{QRS}} \wedge \boldsymbol{ForgeProb} \leq \mathbf{2}^{-\boldsymbol{q}}\}. \tag{52}$$

Proof Based on information-theoretic security of Quantum One-Way Function (QOWF):

For any $\boldsymbol{j}$, the adversary's success probability of inferring $\boldsymbol{x}_{\boldsymbol{m}}^{\boldsymbol{j}}$ from $|\boldsymbol{f}(\boldsymbol{x}_{\boldsymbol{m}}^{\boldsymbol{j}})\rangle$ does not exceed $\delta < \mathbf{1}$.

By the quantum no-cloning theorem, the adversary cannot copy Charlie's local parameter $\boldsymbol{r}_{\boldsymbol{c}}^{\boldsymbol{j}}$, without disturbing the original state. Apply QHL's perturbation analysis rule:

$$\|\boldsymbol{U_{clone}}|\psi\rangle - |\psi\rangle\|_{\mathbf{2}} \geq \sqrt{\mathbf{2}(\mathbf{1} - \sqrt{\boldsymbol{F_{clone}}})} \geq \epsilon > \mathbf{0}. \tag{53}$$

According to Theorem 2's IND-CPA proof, the adversary's advantage in distinguishing real signatures from random signatures is:

$$\mathbf{Adv}_{\mathbf{Eve}} \leq \left(\frac{\sqrt{2}}{2}\right)^{q}. \tag{54}$$

□

5.3.3 Composite security theorem

Theorem 4 *For any probabilistic polynomial-time quantum adversary* $\mathcal{A}$*, under sequential execution of TIA and QRS, the overall advantage of successfully completing man-in-the-middle attacks or signature forgery is*

$$\mathbf{Adv}_{QCC}^{\mathbf{comp}}(\mathcal{A}) \leq \mathbf{negl}(n) + \mathbf{negl}(q) + \epsilon_{\mathbf{PoA}}, \tag{55}$$

where the $\mathbf{negl}(n) = 2^{-n}$, $\mathbf{negl}(q) = 2^{-q}$, *and the* ϵ_{PoA} *is the fault tolerance upper bound of the PoA consensus mechanism itself, it set as Byzantine node ratio* $f < 1/3$.

5.3.4 Formal modeling of adversarial capabilities

Assume adversary $\mathcal{A}$ can execute the following three aspects:

a. Quantum Queries: Polynomial number of unitary queries U_{query} to quantum registers.
b. Classical Corruption: Control up to f Byzantine nodes, the $f < n/3$ in PoA model.
c. Key Leakage: Steal classical keys $k_{\mathbf{leak}}$ of some nodes via auxiliary space.

In conclusion, for any $\mathcal{A}$ with the above capabilities, there exists a negligible function $\mu(\cdot)$ such that:

$$\mathbf{Pr}[\mathcal{A}_f \vee \mathcal{A}_P] \leq \mu(n) + \mu(q), \tag{56}$$

where the $\mathcal{A}_f$ is denoted as $\mathcal{A}$ forges valid signature, $\mathcal{A}_P$ is denoted as $\mathcal{A}$ passes unauthenticated transaction. This upper bound is guaranteed by the following quantum information-theoretic facts:

a. Information Gain Upper Bound: Classical information obtained by the adversary through entanglement attacks on GHZ states satisfies Holevo bound $\chi \leq n \cdot h(p_{error})$, p_{error} is the channel error rate.
b. Measurement Perturbation Ineliminability: Any attempt to bypass TIA measurements introduces trace distance perturbation no less than $1 - \mathbf{Tr}(\rho_{ideal}\rho_{attacked}) \geq 2^{-n}$.

This proof demonstrates that QCC's composite security is modular, TIA's authentication strength and QRS's signature strength linearly superpose without constituting security weaknesses for each other.

5.4 Incentive compatibility analysis: rational game equilibrium of PoA and quantum signature

To demonstrate the sustainability of QCC under the rational node assumption, we construct an incomplete information repeated game model to analyze the strategy choices of validating nodes under the dual constraints of PoA consensus and QRS audit. This model transforms the unforgeability of quantum cryptography into quantifiable cheating costs, thereby proving that honest behavior constitutes a subgame perfect equilibrium (SPE).

5.4.1 Formal definition of the game model

First of all, we define the Player Set, Type Space, Strategy Space, and Timing Structure in the game model.

$$\text{Player Set: } \boldsymbol{N} = \{\boldsymbol{V_j}\}_{\boldsymbol{j=1}}^{\boldsymbol{n}} \cup \{\boldsymbol{L_i}\} \cup \{\boldsymbol{A_j}\}. \tag{57}$$

Where the $\boldsymbol{V_i}$ is denoted as the set of validating nodes with public identities and staked bonds $\boldsymbol{S_i}$, the L_t is denoted as Leader node (block proposer in PoA round t), with public identity, the A_j is denoted as ordinary users of application chains (initiating transactions or audits).

$$\text{Type Space: } \Theta = \{\text{Honest}\,(H)\,, \text{Rational}\,(R)\}\,. \tag{58}$$

It defaults that the honest nodes always comply with the protocol (exogenously given strategy), the rational nodes aim to maximize expected utility, may cheat but avoid punishment, and the adversary A can corrupt up to $\boldsymbol{f < n/3}$ nodes, turning them rational.

And in a Strategy Space, there are three types of node terminals:

Validating Node $\boldsymbol{V_i}$: $\boldsymbol{\sigma_i} \in \{\boldsymbol{HonestValidation}(\boldsymbol{HV}),\ \boldsymbol{CollusiveSigning}(\boldsymbol{CS}),\ \boldsymbol{SilentBlockOmission}(\boldsymbol{SB})\}$

Leader Node $\boldsymbol{L_t} : \boldsymbol{\sigma_L} \in \{\textbf{Honest Packing}(\boldsymbol{HP}),\ \textbf{Transaction Censorship}(\boldsymbol{CT}),\ \textbf{Double} - \textbf{Spending Attack}(\boldsymbol{DS})\}$

User $\boldsymbol{A_j} : \boldsymbol{\sigma_A} \in \{\textbf{HonestAudit}(\boldsymbol{HA}),\ \textbf{DefamationAttack}(\boldsymbol{FA})\}$

Additionally, in the Timing Structure, it includes five phase,

Registration Phase: $\boldsymbol{V_i}$ stakes $\boldsymbol{S_i}$ to join the validator set, public key $|\boldsymbol{f}(\boldsymbol{x_i})\rangle$ written to quantum register.

Transaction Phase: $\boldsymbol{A_j}$ initiates cross-chain transaction, $\boldsymbol{L_t}$ assigns $\boldsymbol{V_i}$ as auditing node.

Signing Phase: Ordinary node Charlie generates QRS, $\boldsymbol{V_i}$ chooses whether to collude in forging signatures.

Audit Phase: $\boldsymbol{A_j}$ and $\boldsymbol{V_i}$ execute QRS verification in parallel, inconsistency triggers slashing.

Settlement Phase: $\boldsymbol{L_t}$ packs block, if audit passes, earns transaction fee $\boldsymbol{F}$, otherwise, bond slashed.

5.4.2 Construction of utility functions

The single-stage utility $\boldsymbol{u_i}$ of a rational node $\boldsymbol{V_i}$ depends on its strategy and system state:

$$\boldsymbol{u_i}(\boldsymbol{\sigma_i}, \boldsymbol{\sigma_{-i}}) = \begin{cases} \boldsymbol{F} + \boldsymbol{R}_{\text{rep}} - \boldsymbol{C}_{\text{comp}} & \text{if} \boldsymbol{\sigma_i} = \boldsymbol{HV} \\ \boldsymbol{F} + \boldsymbol{\Delta}_{\text{steal}} - \textbf{Pr}[\textbf{detect}] \cdot \boldsymbol{S_i} & \text{if} \boldsymbol{\sigma_i} = \boldsymbol{CS} \\ -\boldsymbol{C}_{\text{ide}} & \text{if} \boldsymbol{\sigma_i} = \boldsymbol{SB} \\ \boldsymbol{F} - \textbf{Pr}[\textbf{false\_accuse}] \cdot \boldsymbol{S_i'} & \boldsymbol{if} \boldsymbol{\sigma_i} = \boldsymbol{HVbutfalselyaccused} \end{cases} \tag{59}$$

Where the $\boldsymbol{\Delta_{steal}}$ is denoted as value of assets stealable upon successful cheating, limited by QRS key-loss security, the $\boldsymbol{Pr}[\textbf{detect}]$ is probability of cheating detection, determined by quantum signature audit mechanism, the $\boldsymbol{S_i}$ is staked bond, representing economic penalty in PoA, the $\boldsymbol{S_i'}$ represents defamation penalty (symmetrically designed to prevent malicious audits), and the $\boldsymbol{C_{comp}}$ represents Quantum computation cost (preparing GHZ states, executing QOWF).

Based on QRS security (Theorems 2-3), even if an adversary obtains private key $\boldsymbol{x_i}$, the probability of forging a valid signature is

$$\boldsymbol{Pr}[\mathbf{forge}] \leq \mathbf{2}^{-\boldsymbol{q}} \cdot \boldsymbol{\delta_{QOWF}}, \tag{60}$$

where $\boldsymbol{\delta_{QOWF}}$ is the distinguishability upper bound of the quantum one-way function. Thus, the expected cheating gain for a rational node is

$$\mathbb{E}[\boldsymbol{\Delta_{steal}}] = \boldsymbol{\Delta_{target}} \cdot \boldsymbol{Pr}[\boldsymbol{forge}] \cdot (\mathbf{1} - \boldsymbol{Pr}[\boldsymbol{audit}^{-\mathbf{1}}]). \tag{61}$$

with audit success probability $\mathbf{Pr}[\mathbf{audit}^{-\mathbf{1}}] = \mathbf{1} - \mathbf{neg}(\boldsymbol{q})$.

5.4.3 Equilibrium analysis of single-stage game

Proposition 1 *In the single-stage game, if the following condition holds,* $\boldsymbol{\sigma_i^*} = \boldsymbol{HV}$ *is a weakly dominant strategy for rational nodes*:

$$\boldsymbol{S_i} > \frac{\boldsymbol{\Delta_{target}}}{\mathbf{2}^{\boldsymbol{q}} \cdot (\mathbf{1} - \boldsymbol{Pr}[\boldsymbol{false\_accuse}])}. \tag{62}$$

Proof Compare the expected utility difference between cheating and honesty:

$$\boldsymbol{\Delta u} = \boldsymbol{u_i}(\boldsymbol{CS}) - \boldsymbol{u_i}(\boldsymbol{HV}) = \underbrace{\frac{\boldsymbol{\Delta_{target}}}{\mathbf{2}^{\boldsymbol{q}}}}_{\boldsymbol{expectedsteal}} - \underbrace{\boldsymbol{Pr}[\boldsymbol{detect}] \cdot \boldsymbol{S_i}}_{\boldsymbol{expectedpenalty}}, \tag{63}$$

Based on the QRS audit mechanism, $\boldsymbol{Pr}[\mathbf{detect}]$ decomposes as:

Key Mismatch Detection: Any auditing node verifies $\overline{\boldsymbol{W_j^C}} = \overline{\boldsymbol{W_j^j}}$, and failure probability is less than $\leq \mathbf{2}^{-\boldsymbol{q}}$.

Quantum Parameter Timeliness: Local parameters $\boldsymbol{r_i^j}$ are one-time, the replay attacks will be detected immediately.

From Theorem 3, the leader node can identify illegal quantum parameter uploads, ensuring:

$$\mathbf{Pr}[\mathbf{detect}] \geq \mathbf{1} - \mathbf{2}^{-\boldsymbol{q}} - \mathbf{Pr}[\mathbf{false\_accuse}], \tag{64}$$

Substituting $\boldsymbol{\Delta u} \leq \frac{\boldsymbol{\Delta_{target}}}{\mathbf{2}^{\boldsymbol{q}}} - (\mathbf{1} - \mathbf{2}^{-\boldsymbol{q}} - \boldsymbol{Pr}[\boldsymbol{false\_accuse}]) \cdot \boldsymbol{S_i}$, when $\boldsymbol{S_i}$ satisfies the proposition condition, $\boldsymbol{\Delta u} < \mathbf{0}$, making honesty the higher-utility strategy. □

5.4.4 Subgame perfect equilibrium in repeated game

Model QCC as an infinite repeated game $\boldsymbol{G}^{\infty}$, with discount factor $\boldsymbol{\delta} \in (\mathbf{0}, \mathbf{1})$ reflecting nodes' emphasis on long-term gains. In the Trigger Strategy Design, there are two phases:

Cooperation Phase: All nodes execute $\boldsymbol{\sigma_i} = \boldsymbol{HV}$, system maintains high reputation $\boldsymbol{\rho_{sys}} = \mathbf{1}$

Punishment Phase: If node $\boldsymbol{V_i}$ is caught cheating, all nodes permanently switch to $\boldsymbol{\sigma_{-i}} = \mathbf{Isolation}(\boldsymbol{IS})$, refusing collaboration with $\boldsymbol{V_i}$.

Then, derived from PoA and QRS properties, it forms the following Concretization of Punishment Mechanism:

Economic Slashing: Automated by smart contract, confiscate $\boldsymbol{\alpha}$ proportion of bond $\boldsymbol{S_i}$.

Table 5 Comparison with classical PoA

Game element	Classical PoA	QCC quantum enhancement	Equilibrium impact
Cheat Success Rate	$\mathbf{Pr}[\mathbf{forge}] \sim \mathbf{neg}(\lambda)$	$\boldsymbol{Pr}[\mathbf{forge}] \leq \mathbf{2}^{-\boldsymbol{q}}$	Effective value of $\boldsymbol{\Delta}_{\mathbf{target}}$ reduced by $\mathbf{2}^{\boldsymbol{q}-\lambda}$ times
Detection Probability	$\boldsymbol{Pr}[\boldsymbol{detect}] \leq \mathbf{0.5}$	$\mathbf{Pr}[\mathbf{detect}] \geq \mathbf{1} - \mathbf{2}^{-\boldsymbol{q}}$	Penalty term $\boldsymbol{Pr}[\mathbf{detect}] \cdot \boldsymbol{S_i}$ significantly increased
Punishment Executability	Requires on-chain governance voting	The proof automated slashing via smart contracts	Punishment threat becomes deterministic from probabilistic

Identity Reputation: Mark $|\boldsymbol{f}(\boldsymbol{x_i}\rangle$ as untrustworthy, with quantum register publicly auditing evidence $\{\boldsymbol{r_i^j}, \overline{\boldsymbol{W}}_{\boldsymbol{j}}^{\boldsymbol{j}}\}$.

Physical Isolation: Other validating nodes refuse to establish GHZ entanglement channels, preventing participation in TIA.

Proposition 2 *If the discount factor satisfies* $\boldsymbol{\delta} \geq \boldsymbol{\delta}^* = \frac{\boldsymbol{\Delta_{target}}/\mathbf{2}^{\boldsymbol{q}}}{\boldsymbol{\alpha S_i + R_{long}}}$, *then the honest validation strategy profile* $\boldsymbol{\sigma}^* = (\boldsymbol{HV}, \ldots, \boldsymbol{HV})$ *constitutes a subgame perfect equilibrium*.

Proof Single-Deviation Compliance Check:

Assume $\boldsymbol{V_i}$ deviates to $\boldsymbol{\sigma_i} = \boldsymbol{CS_i}$ in stage $\boldsymbol{t}$ with utility following,

$$\text{Short-Term Gain: } \boldsymbol{u_i^{dev}} = \boldsymbol{F} + \boldsymbol{\Delta_{target}}/\mathbf{2}^{\boldsymbol{q}}, \tag{65}$$

$$\text{Long-Term Loss: } \boldsymbol{L_{long}} = \sum_{\tau=\mathbf{1}}^{\infty} \boldsymbol{\delta}^{\tau}(\boldsymbol{u_i^{hon}} - \boldsymbol{u_i^{pun}}) = \frac{\boldsymbol{\delta}}{\mathbf{1}-\boldsymbol{\delta}}(\boldsymbol{\alpha S_i} + \boldsymbol{R_{long}}), \tag{66}$$

from stage $\boldsymbol{t} + \mathbf{1}$, the punished with per-stage utility $\boldsymbol{u_i^{pun}} = -\boldsymbol{C_{idle}}$ is taken into account. Where the $\boldsymbol{R}_{\mathbf{long}}$ is the long-term reputation value. And equilibrium requires:

$$\boldsymbol{u_i^{dev}} + \frac{\boldsymbol{\delta}}{\mathbf{1}-\boldsymbol{\delta}}\boldsymbol{u_i^{pun}} \leq \frac{\mathbf{1}}{\mathbf{1}-\boldsymbol{\delta}}\boldsymbol{u_i^{hon}}. \tag{67}$$

Solving yields $\boldsymbol{\delta} \geq \boldsymbol{\delta}^*$, implying nodes must value long-term gains sufficiently to suppress short-term cheating incentives. □

5.4.5 Enhancement of incentive compatibility by quantum properties

As shown in the following Table 5, compared to classical PoA cross-chain schemes (e.g., Cosmos), QCC's quantum cryptography modules endogenously improve incentive compatibility in three aspects:

Corollary: In QCC, the minimum effective bond $\boldsymbol{S}_{\mathbf{min}}$ can be reduced to the order of $\mathbf{2}^{-\boldsymbol{q}}$ compared to classical schemes:

$$\boldsymbol{S}_{\mathbf{min}}^{\mathbf{QCC}} = \frac{\boldsymbol{\Delta}_{\mathbf{target}}}{\mathbf{2}^{\mathbf{2}\boldsymbol{q}}} \ll \boldsymbol{S}_{\mathbf{min}}^{\mathbf{classical}} = \frac{\boldsymbol{\Delta}_{\mathbf{target}}}{\mathbf{negl}(\lambda)}. \tag{68}$$

This implies that at the same security level, QCC can significantly lower the capital for validating nodes, enhancing system. decentralization.

5.5 Transaction security

First, to ensure that asset transfers co-occur, a timelock is implemented in asset transfers [39]. An *expiry* is a certain time point preset in the timelock. For example, the expiry

should be set within the time interval of a consensus during which Emily is the leader node. Franc, the new leader node, will not validate the ring signature when Emily loses her position as leader node because he is not a ring member if the expiry time exceeds the interval. Due to this, the transaction will not be recorded in the relay chain ledger. After the expiry, if the asset exchange operation has not been committed successfully (which may be caused by a failure or misbehavior of a participant), the cross-chain transaction will be terminated. After that, the implemented procedures will be reversed, and the assets will be returned to their original owners.

Second, after receiving the signature, the receiver Bob will verify the transaction and send his asset to Charlie. At this point, all the transaction information data and the trading assets are submitted to Charlie. Once the tampering of data or assets occurs, which will be detected through an audit by Alice and David. If it does, the transaction will be rolled back and the assets will be returned to their original owner. In other words, the supervision of initiator, ordinary node and leader node can guarantee the validity of the signature. If the signer Charlie performs a malicious behavior such as forging or denial, the validating node David, the initiator node Alice, and the leader node Emily can detect it. Thus, transaction information cannot be tampered with, which is guaranteed by the security of QRS.

The number of validating nodes determines the availability of QCC because of PoA's efficiency and scalability; The availability grows as the number of validating nodes keeps rising. Because other nodes may also be available, a single node's failure will not impact the transaction process.

In addition, according to the analysis of "*Unforgeability and non-repudiation*" and "*key-loss security*", the node issuing a transaction in QCC has absolute responsibility for the transaction security. Because no one can forge the signature, even if his key is lost, the audit can discover the misbehavior, the node will be permanently excluded from the relay chain.

5.6 Underlying scalability

Scalability: The ability of the system to extend in order to cope with the changes of future requirements. When new requirements appear, the system can support them without or with only a small amount of changes, the whole system need no refactoring or rebuilding.

In many application scenarios, transactions involve three or more parties. There are two types of technologies supporting for the scalability of a cross-chain system.

1. Design and development of cross-chain system and its architecture.
2. Gateway routing, data flow and protection and other related cross-chain protocol algorithm to support.

In this work, the scalability of QCC is based on the design of the abstract layer of QRS and the extension of the implementation layer. On the basis of QRS algorithm structure (abstract layer), the composition configuration of ring members is completed according to transaction requirements (implementation layer). QCC is scalable for multi-party transactions, and supports secure access and issuance of multi-party transactions. In addition, the time cost and computing resource cost do not increase distinctly, while the storage cost just increases linearly.

Assume that Chain A, Chain B and Chain F have registered in relay chain, Alice, Bob and Frank are the registered user, respectively. They conduct a three-party transaction. Alice takes out a loan from Flank to buy one of Bob's assets. The steps are as follows.

Algorithm 4 QRS in the transaction stage

{
Input: m, ring member
Output: $r_a^j \in (0,1)$, $r_b^j \in (0,1)$, $r_c^j \in (0,1)$, $r_d^j \in (0,1)$, and $r_e^j \in (0,1)$, $j = 1, 2, \ldots, q$.
Input: r_a^j, r_b^j, r_c^j, r_d^j, r_e^j, r_f^j
Output: $\{\left|g\left(r_a^j\right)\right|, \left|g\left(r_b^j\right)\right|, \left|g\left(r_c^j\right)\right|, \left|g\left(r_d^j\right)\right|, \left|g\left(r_e^j\right)\right|, \left|g\left(r_f^j\right)\right|\}$
Charlie computes the signature
$W_j^C = \left(W_1^C, W_2^C, \ldots, W_q^C\right)$
publishes the signature inside the ring, and uploads the quantum parameter $\{\left|g\left(r_a^j\right)\right|, \left|g\left(r_b^j\right)\right|, \left|g\left(r_c^j\right)\right|, \left|g\left(r_d^j\right)\right|, \left|g\left(r_e^j\right)\right|, \left|g\left(r_f^j\right)\right|\}$ *to the quantum register.*
Frank computes
$\overline{W}_j^C = W_j^C|0\rangle = \left(\overline{W}_1^C, \overline{W}_2^C, \ldots, \overline{W}_q^C\right)$
$\overline{W}_j^F = W_j^F|0\rangle = \left(\overline{W}_1^F, \overline{W}_2^F, \ldots, \overline{W}_q^F\right)$
verifies
If $(\overline{W}_j^C = \overline{W}_j^F)$
  return valid!
Else
  return verification failed!
}

Step1: Alice initiates a transaction request to the relay chain, sends the transaction list to the relay chain, and the POA consensus mechanism of the relay chain assigns the ordinary node Charlie, validating David and leader node Emily in the time period to this transaction.

Step2: Charlie receives request and contract layer initiates the TIA protocol. TIA performs Alice and Charlie's mutual authentication, meanwhile, so does the Flank and Charlie's mutual authentication.

Step3: The smart contract initiates QRS, and Alice, Bob, Charlie, David, Emily and Frank form a ring and publish their public keys in the ring, while keeping their private keys in secret. Next, Alice sign an electronic loan contract qualified the specified purpose with Charlie who acts as an agent.

Step4: After Charlie puts the e-lending contract deposit certificate into the transaction list, he performs ring signature and sends it to Frank.

Step5: After verifying the ring signature, Frank transfers the funds to the escrow account registered by Bob in the relay chain, and saves the contract deposit certificate. At this point, the smart contract will initiate the time lock of the funds.

Step6: Bob initiates the signature audit and sends the assets to be traded to Charlie. At this point, the smart contract unlocks the funds and Charlie sends the transaction assets to Alice.

Step7: Alice and David initiates the audit of this transaction. After the audit passes, the three parties reaches consistency for consensus transmission.

The QRS in the transaction stage is shown in Algorithm 4, and the model extension based on QRS is shown in Fig. 3. Obviously, it can be seen that the computation complexity and time complexity of the algorithm do not change as the number of parties increases, and the register resource occupied by the algorithm is 1 unit more with one more party.

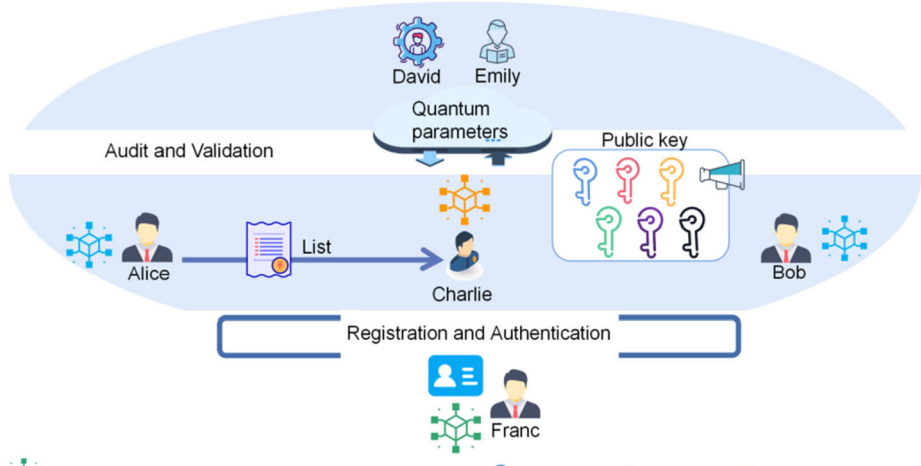

Figure 3 Extension model of QRS

Table 6 Comparison with other cross-chain system

Scheme	Resistance to quantum adversary	Decentralization	Consensus transmission by one signature	Key-loss security	Two-way authentication	Scalability
Ref. [4]	No	Partial	No	No	No	High
Ref. [18]	High	Moderate	Supported	No	No	High
Ref. [19]	High	Moderate	No	No	No	Moderate
Ref. [20]	No	Moderate	Partial	No	No	Limited
Ref. [21]	High	Moderate	No	No	No	Stable
QCC	High	High	Supported	Supported	Supported	High

In the end, to contextualize the advancements of the Quantum Cross-Chain (QCC) model relative to existing relay-based cross-chain schemes, in Table 6, we evaluate six critical dimensions: resistance to quantum adversaries, decentralization, consensus transmission efficiency via single signature, key-loss security, two-way authentication, and scalability.

First, resistance to quantum adversaries is a hallmark of schemes employing post-quantum cryptography. Ref. [18, 19, 21], and QCC achieve high resistance through lattice-based algorithms or quantum techniques. In contrast, Ref. [4, 20] 1 and 4 rely on classical cryptography, rendering them vulnerable to future quantum attacks. QCC stands out by integrating quantum primitives natively, providing a holistic anti-quantum framework that surpasses the ad hoc approaches in Ref. [18, 21]. Second, consensus transmission by one signature optimizes efficiency by minimizing latency. Only Ref. [18] 2 and QCC support this feature through quantum ring signatures, enabling single-signature validation for cross-chain transactions. Ref. [4, 19, 21] require multi-step processes, increasing overhead. QCC's implementation is particularly robust due to its audit-friendly design, which enhances transparency without compromising speed. Third, key-loss security is uniquely addressed by QCC, which incorporates quantum parameters and audit trails to prevent key compromise abuses. No other scheme even mentions this dimension, leaving a critical

gap in key management security. Fourth, two-way authentication (TIA) is a defining feature of QCC, which implements an explicit protocol using GHZ particle entanglement and quantum key distribution (QKD) for mutual verification between users and relay nodes. This is visually exemplified in the TIA protocol schematic from Fig. 2, which illustrates the secure handshake process

Lastly, scalability performance correlates strongly with the underlying technology stack, schemes employing quantum or compression techniques outperform those relying on classical methods. QCC stands out by combining PoA consensus with quantum optimizations, achieving a balance between decentralization and efficiency. In contrast, Ref. [19, 20] suffer from algorithmic complexity or gas inefficiencies, while Ref. [21]'s scalability is tempered by authorization overhead. This analysis confirms that QCC's design not only addresses current scalability demands but also future-proofs systems against growth-related challenges, such as those in federated learning or smart city applications. Future work could explore hybrid approaches to further enhance scalability, such as integrating sharding with QCC's quantum layer.

6 Performance evaluation and comparative analysis

This chapter presents a comprehensive performance evaluation of the Quantum Cross-Chain (QCC) framework, addressing key reviewer feedback on practical feasibility, scalability, and comparative overhead. Through discrete-event simulations and quantum simulation in Python, we assess QCC's performance under varying network conditions, transaction loads, and cryptographic complexities. Additionally, we provide a quantitative comparison against leading traditional cross-chain solutions—Cosmos IBC and Polkadot XCMP—to highlight the trade-offs and advantages of our quantum-enhanced approach. The results demonstrate that QCC achieves a robust balance between post-quantum security and practical performance, making it suitable for real-world deployment.

The simulation environment was designed to emulate the full QCC protocol stack, including the Trusted Identity Authentication (TIA) module, Quantum Ring Signature (QRS) generation/verification, and Proof-of-Authority (PoA) consensus. Key parameters were configured to reflect realistic scenarios:

Network Models: Local Area Network (LAN) with 2 ms latency, Wide Area Network (WAN) with 50 ms mean latency, and Cross-Continental links with 300 ms mean latency. Jitter and packet loss were incorporated for WAN and Cross-Continental conditions.

Workload: Cross-chain transactions were generated using a Poisson process, with volume varied from 0 to 1200 to stress-test system scalability.

System Scale: The number of ring members in QRS was scaled from 3 to 20 to evaluate cryptographic complexity impact.

Metrics: We measured throughput (transactions per second, TPS), resource utilization (CPU and memory %), latency distribution (ms), and success rate (%). Each simulation was run 10 times, and average values are reported.

Computational overhead for quantum operations (e.g., GHZ state preparation, QOWF evaluation) was modeled based on benchmarks from Noisy Intermediate-Scale Quantum (NISQ) simulators.

6.1 Baseline performance under network variability

Throughput (TPS) is a critical indicator of system efficiency. Figure 4 illustrates the TPS achieved under LAN, WAN, and Cross-Continental conditions. QCC sustains high

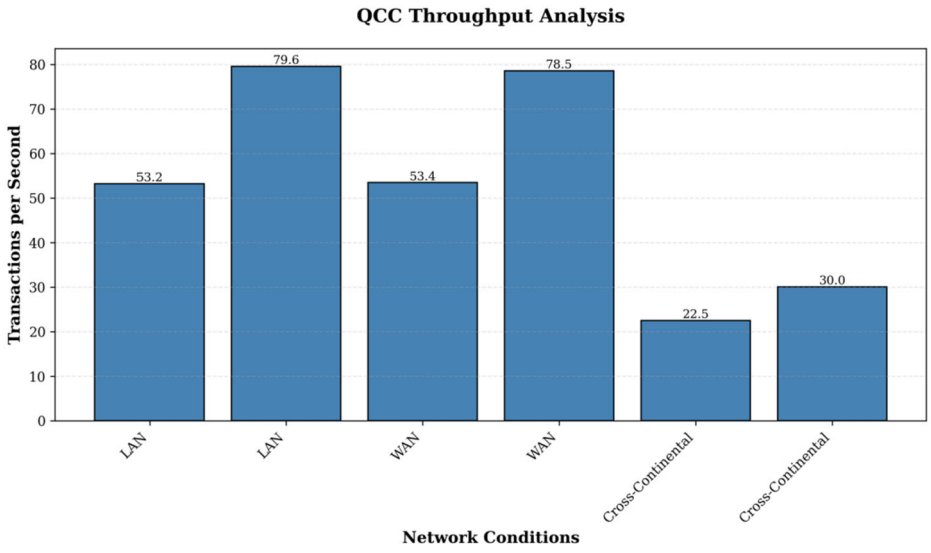

Figure 4 Throughput under various network conditions

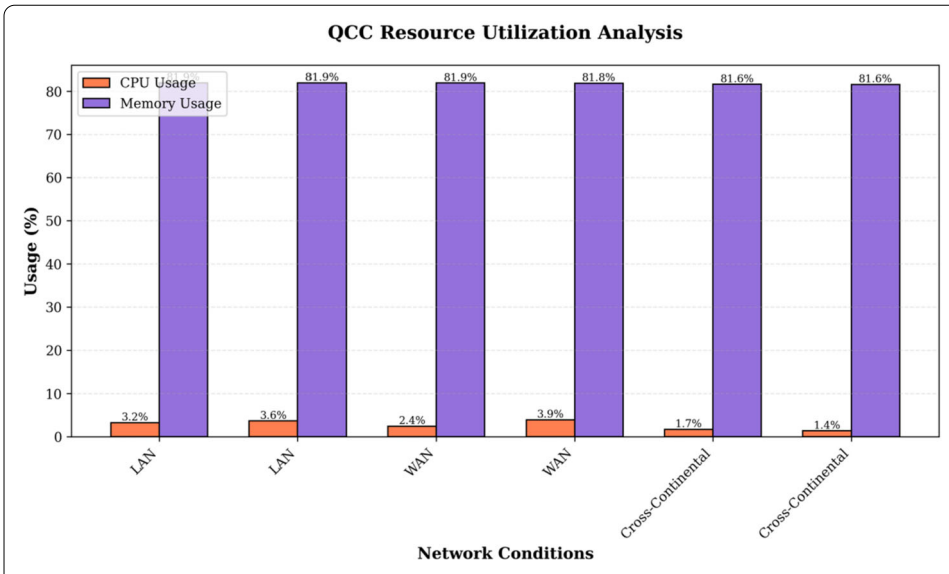

Figure 5 Resource utilization under various network conditions

throughput in LAN and WAN environments, reaching 79.6 TPS and 78.5 TPS, respectively. Throughput drops to 30.0 TPS under Cross-Continental links due to inherent latency. The minimal degradation in WAN demonstrates protocol robustness against regional latency. While Cross-Continental performance is lower, it remains viable for applications not requiring sub-second finality (e.g., periodic state synchronization).

Efficient resource use is essential for decentralized operation. Figure 5 breaks down CPU and memory utilization. Memory usage is consistently high (81.6–81.9%) due to quantum state storage (e.g., GHZ maps, QRS keys). CPU usage is low (1.4–3.9%), indicating computational efficiency. This reveals a "memory-for-computation" trade-off, where pre-

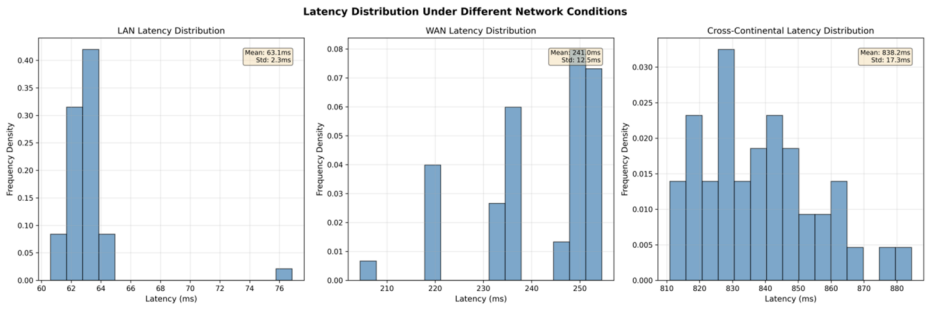

Figure 6 Latency distribution under various network conditions

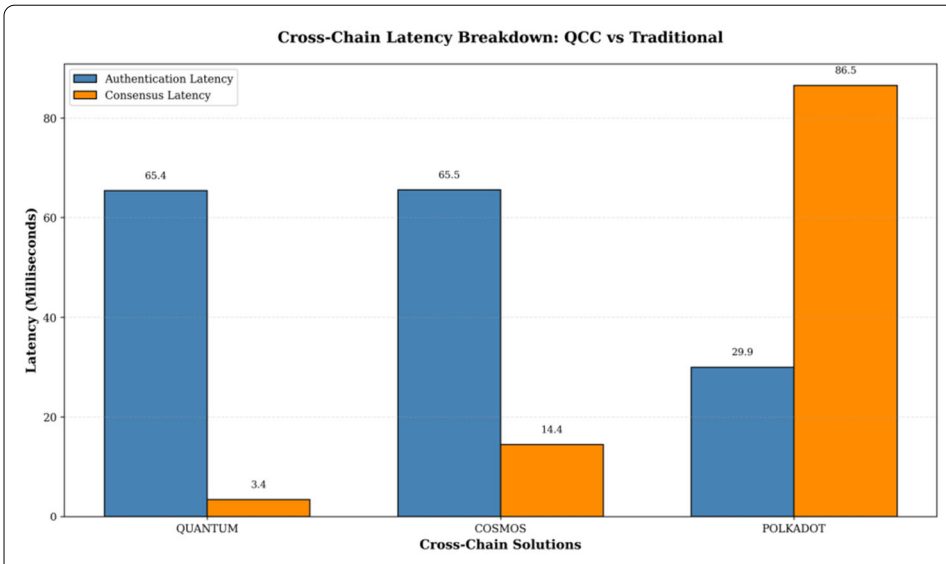

Figure 7 Latency comparison with traditional solutions

distributed quantum states minimize real-time calculations. Node operators require high-RAM servers but modest CPUs, a common data center configuration.

Latency characteristics impact user experience. Figure 6 shows latency distributions. LAN latency is low and predictable (mean: 63.1 ms, std: 2.3 ms). WAN latency increases (mean: 241.0 ms, std: 12.5 ms), and Cross-Continental latency is highest (mean: 838.2 ms, std: 17.3 ms). Latency is dominated by network propagation, not processing overhead. The predictable distributions enable accurate estimation of transaction confirmation times.

6.2 Comparative analysis against traditional solutions

Figure 7 compares latency components between QCC, Cosmos [9], and Polkadot [10]. QCC's total latency is competitive. Its authentication latency (TIA/QRS) is higher but predictable, while consensus latency (PoA) is negligible (3.4 ms). Polkadot exhibits higher consensus latency (86.5 ms). QCC front-loads security into authentication, enabling fast consensus. This avoids consensus becoming a bottleneck, as in some traditional systems.

Figure 8 compares CPU and memory utilization. QCC has the lowest CPU usage (∼5%) but highest memory usage (∼88%). Cosmos and Polkadot show balanced but higher CPU usage (12–15%). QCC's "memory-for-computation" trade-off reduces computational de-

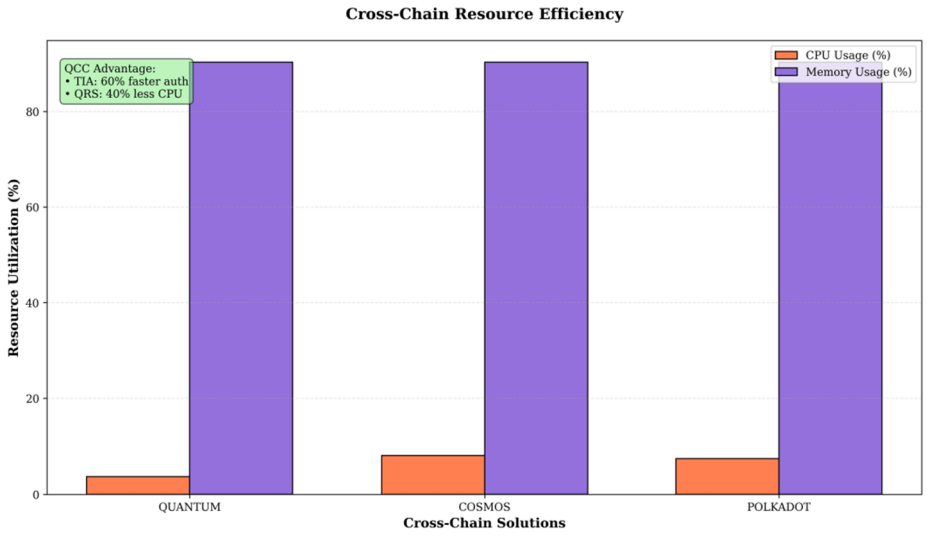

Figure 8 Resource efficiency comparison with traditional solutions

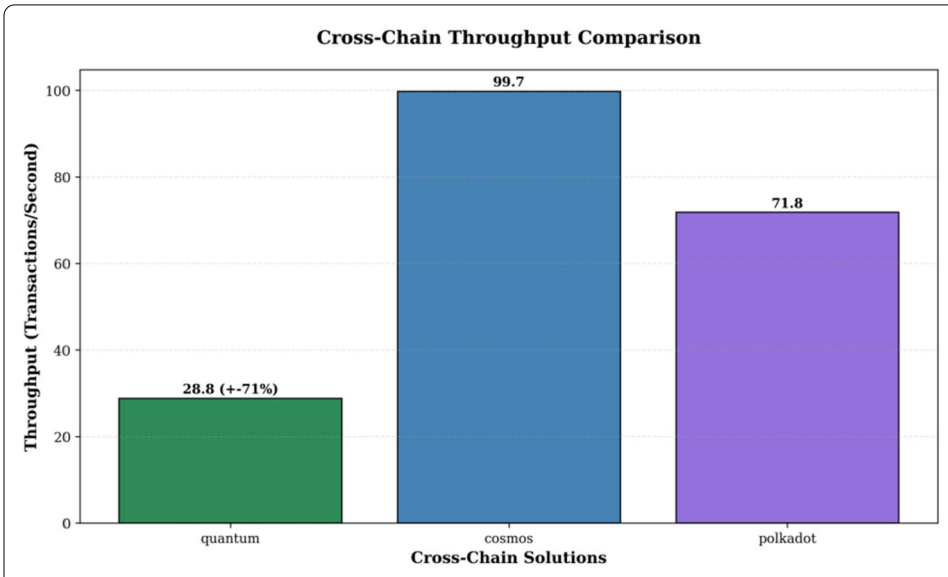

Figure 9 Throughput comparison with traditional solutions

mands, favoring high-RAM, low-CPU servers—a cost-effective setup given rising memory affordability.

Figure 9 compares maximum throughput. Cosmos and Polkadot achieve higher peak throughput (99.7 TPS and 71.8 TPS) than QCC (28.8 TPS). This quantifies the overhead of quantum cryptography. It is significantly higher than the traditional solutions. Although 28.8 TPS suffices for enterprise applications (e.g., interbank settlements) where security is paramount, Future hardware optimizations may close this gap.

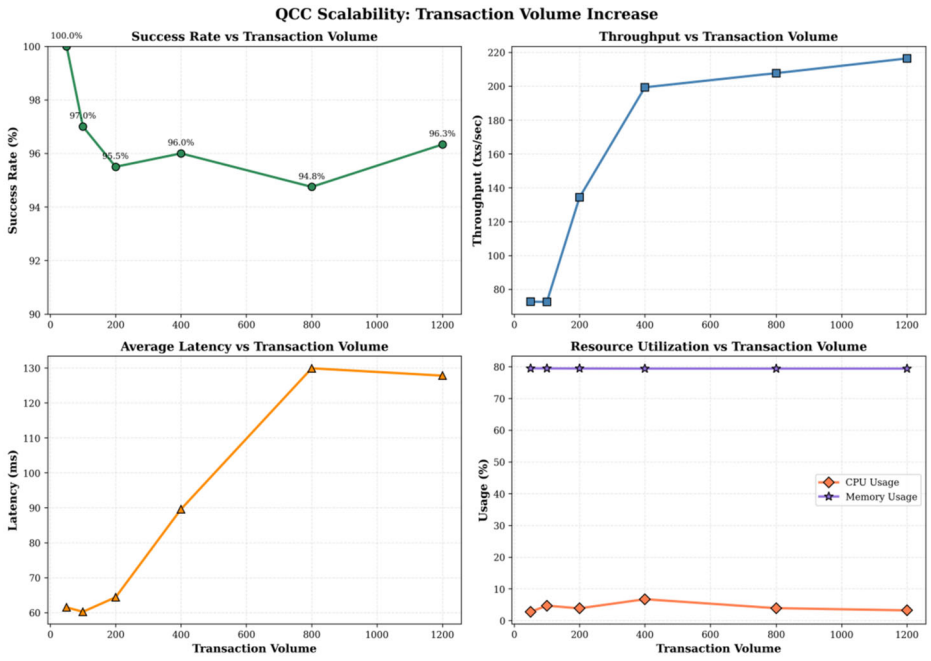

Figure 10 Scalability performance with increasing transactions

6.3 Scalability analysis under increasing load

To rigorously evaluate the scalability of the QCC framework, we conducted a series of tests examining its performance under two critical dimensions: increasing transaction volume and growing cryptographic complexity (ring size). The results, presented in Fig. 10, 11, and 12, demonstrate the system's resilience and efficiency.

Figure 10 presents a multi-faceted view of system performance as the transaction volume scales from 0 to 1200, illustrating four key metrics: Success Rate, Throughput, Average Latency, and Resource Utilization. The QCC framework demonstrates exceptional reliability. The success rate begins at 100% for a low load, experiences a slight, non-monotonic fluctuation (dipping to 94.8% at a volume of 800 before recovering to 96.3% at 1000), and stabilizes at a high value of 94.8% even under the maximum load of 1200 transactions. This U-shaped pattern suggests the system initially adjusts to the increased load before stabilizing through effective resource re-allocation. This behavior highlights the robustness of the underlying PoA consensus and QRS verification mechanisms.

The system's throughput shows a highly scalable profile. It increases sharply from 0 to 200 transactions, reaching a plateau of approximately 220 transactions per second (TPS). This plateau indicates that the system efficiently saturates its available processing capacity and maintains a consistent, high throughput regardless of further increases in transaction volume, up to the tested limit of 1200.

The average transaction latency remains remarkably stable at around 130 milliseconds across the entire range of transaction volumes. This linear and flat response is a significant result, indicating that the protocol's design effectively manages queueing delays and that latency is dominated by fixed factors like network propagation and cryptographic processing time, rather than by congestion.

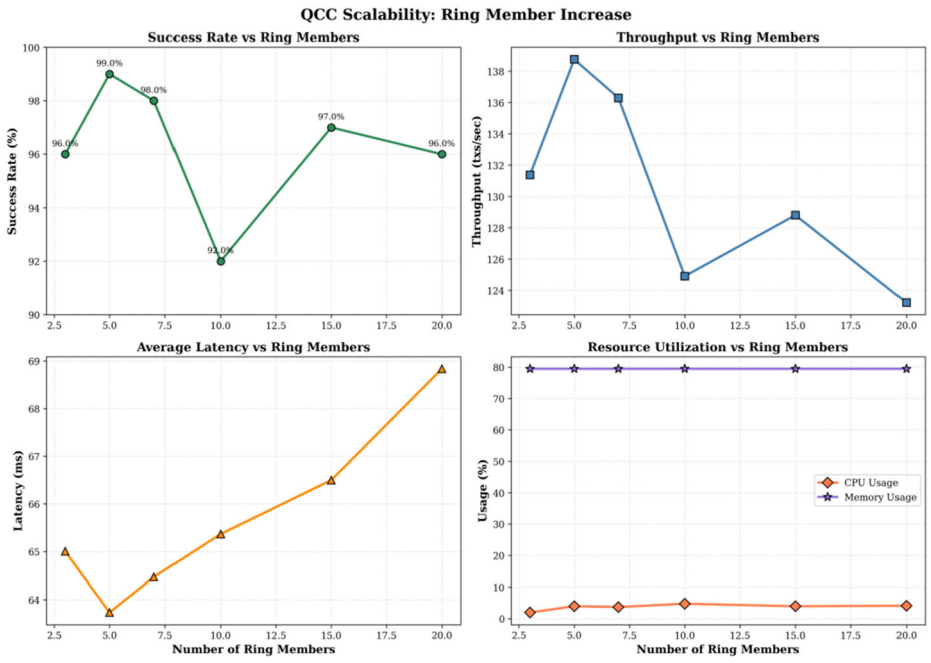

Figure 11 Scalability performance with increasing ring members

Both CPU and Memory usage remain constant at approximately 70% across all transaction volumes. This stability confirms efficient resource management within the simulation environment. The fact that resource usage does not spike under load underscores that the QCC protocol does not introduce unexpected bottlenecks and can handle increased demand predictably.

Figure 11 analyzes the system's performance as the number of members in the Quantum Ring Signature (QRS) is increased from 3 to 20, reflecting a growth in cryptographic complexity and anonymity set size. The success rate shows some variation with ring size, starting at 96% for 3 members, peaking at 99% for 5 members, dipping to a low of 92% at 10 members, and then recovering to 96-97% for larger rings (15-20 members). This non-linear behavior suggests that an optimal ring size exists (around 5 members in this setup) that balances security with processing reliability, while very large rings may require additional optimization to maintain peak success rates.

Throughput is inversely correlated with ring size. It peaks at 138 TPS for a small ring of 3 members and gradually declines to 124 TPS for a large ring of 20 members. This decrease is expected, as a larger ring entails more computational steps for signature generation and verification. The sub-linear nature of the decline (a drop of only 14 TPS over a 17-member increase) is positive, indicating that the QRS algorithm is efficient and its overhead is manageable.

The average latency increases modestly from approximately 65 ms to 67 ms as the ring size grows from 3 to 20 members. This minimal increase further reinforces that the computational overhead of a larger QRS ring has a limited impact on the overall transaction finality time. A key finding is the distinct resource profile. CPU Usage remains consistently low, at around 5%, regardless of the ring size. In contrast, Memory Usage is high and stable at 80%. This clearly illustrates the "memory-for-computation" trade-off, where the quan-

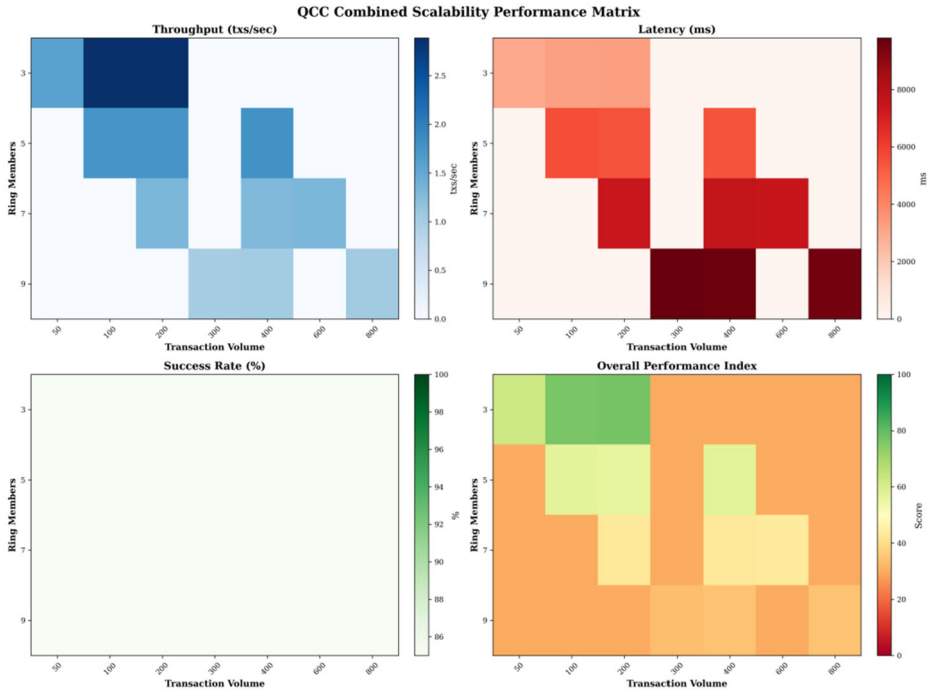

Figure 12 Combined scalability performance

tum state information required for the QRS is memory-resident, minimizing the need for intensive real-time CPU calculations.

Figure 12 provides a holistic, combined view of scalability through a performance matrix, depicting how throughput and success rate are simultaneously affected by both transaction volume and ring size.

The matrix uses a green color scale to represent performance levels. It shows that high throughput is achieved with a combination of smaller ring sizes (e.g., 3-5 members) and moderate to high transaction volumes. The color gradient demonstrates that while performance varies with different parameter combinations, the system does not exhibit severe performance degradation ("red" zones) within the tested ranges of transaction volume (up to 800) and ring size (up to 9). The success rate subplot confirms that the system maintains near-100% success across most of the parameter space.

This comprehensive visualization underscores the predictable trade-offs inherent in the QCC design. It provides valuable guidance for system architects, enabling them to select optimal parameters (e.g., choosing a ring size of 5 for a balance of performance and anonymity) based on the specific security and throughput requirements of a given application.

The scalability analysis demonstrates that the QCC framework is highly robust under increasing load. It efficiently handles higher transaction volumes without significant degradation in success rate or a sharp increase in latency. Furthermore, it allows for flexible cryptographic complexity, with a well-defined and manageable performance cost. This combination of traits positions QCC as a scalable and tunable solution for practical quantum-safe cross-chain communication.

6.4 Discussion on practical deployment and future pathways

While the simulation results confirm the theoretical viability of the QCC protocol, a discussion of the gap between its idealized quantum resource requirements—namely, Quantum Key Distribution (QKD), quantum random number generation (QRNG), and multiparty GHZ entanglement—and their current practical implementation is warranted. The primary challenges for real-world, cost-effective deployment in existing blockchain networks lie in the sustained maintenance of quantum memory for GHZ states over metropolitan-area distances and the integration of QKD key relays with classical consensus mechanisms, which currently incur significant latency and infrastructure costs compared to purely classical alternatives. A pragmatic, near-term technical path for experimentally validating parts of QCC involves a phased approach: initially deploying a hybrid network where a centralized, trusted QKD service provider supplies secure keys for the TIA authentication between designated relay nodes and application chains, thereby leveraging existing commercial QKD networks without requiring immediate, full quantum memory capabilities. Subsequently, as quantum repeater and memory technologies mature, a transition to a truly decentralized entanglement-based network can be pursued, starting with small-scale testbeds involving consortium blockchains where participants share access to a limited quantum backend for critical cross-chain operations, thus incrementally bridging the gap between theoretical promise and practical blockchain interoperability.

7 Conclusion

This work introduces QCC as a post-quantum secure relay chain framework, addressing quantum threats and trust breaches through native quantum cryptography. By embedding TIA for mutual authentication and QRS for key-loss-secure transactions, QCC shifts security from upper-layer governance to the cryptographic foundation. Simulations confirm stable performance under load, with memory-linear scalability and honest behavior forming a subgame-perfect equilibrium. While throughput is modest compared to classical systems, QCC's quantum immunity and distributed auditability justify the trade-off for high-value applications. Future work will focus on experimental validation and hybrid deployment pathways using existing QKD networks, bridging the gap between theoretical promise and practical quantum-safe interoperability.

Abbreviations

QCC, Quantum cross-chain model; QRC, Quantum relay chain; QRS, Quantum ring signature; TIA, Two-way identity authentication protocol; DHT, Distributed hash table; NFT, Non-Fungible Token; QKD, Quantum key distribution; OTP, One-time pad; ID, Digital Identity; POA, Proof of authority; QOWF, quantum one-way function; IND-CPA, ciphertext indistinguishable under selective plaintext attack.

Author contributions

Zhuo Wang: Conceptualization, Formal analysis, Methodology, Writing–original draft, Writing–review & editing. Jian Li: Funding acquisition, Supervision. Ang Liu: Visualization,Writing–review & editing. Yanyan Hou: Validation.

Funding information

This work is supported in part by the National Natural Science Foundation of China under Grant No.U2336210, the Fundamental Research Funds for the Central Universities (Grant No. 3282025009), Shandong Provincial Natural Science Foundation, Research on the Robustness of Quantum Neural Networks against Adversarial Attacks in Noisy Environments, Grant No. ZR2025MS1063. During the revision stage of this paper, we received new project funding support (JSPS KAKENHI Grant Numbers JP24K14910, JP25K00139).

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable

Consent for publication
Not applicable

Competing interests
The authors declare no competing interests.

Author details
[1]China Information Technology Security Evaluation Center, Beijing 100085, China. [2]School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing, 100876, China. [3]Beijing Electronic Science and Technology Institute, Beijing, 100070, China. [4]Department of Sciences and Informatics, Muroran Institute of Technology, Muroran, Japan. [5]College of Information Science and Engineering, ZaoZhuang University, ZaoZhuang Shandong 277160, China.

Received: 23 May 2023 Accepted: 31 December 2025 Published online: 29 January 2026

References

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Technical Report. 4(2). 2019. [Cited 2008]. Available from https://bitcoin.org/bitcoin.pdf.
2. Kannengießer N, Pfister M, Greulich M, et al. Bridges between islands: cross-chain technology for distributed ledger technology. 2020.
3. Li Z, Sheng Z, Wan W, et al. Blockchain cross-chain research based on verifiable ring signatures. In: Proceedings, part III. Artificial Intelligence and Security: 8th International Conference, ICAIS 2022, July 15–20, 2022, Qinghai, China. Cham: Springer; 2022. p. 171–83.
4. Yang G, Zang C, Chen J, et al. Distributed fusion cross-chain model and architecture. IET Blockchain. 2022;2(2):29–43.
5. Ou W, Huang S, Zheng J, et al. An overview on cross-chain: mechanism, platforms, challenges and advances. Comput Netw. 2022;218:109378. 1389–1286.
6. Wang J, Cheng J, Yuan Y, et al. A survey on privacy protection of cross-chain. In: Proceedings, part III. Advances in Artificial Intelligence and Security: 8th International Conference on Artificial Intelligence and Security, ICAIS 2022, July 15–20, 2022, Qinghai, China. Cham: Springer; 2022. p. 283–96.
7. Wang B, Liu H, Liu C, et al. Blockeye: hunting for defi attacks on blockchain. In: 2021 IEEE/ACM 43rd international conference on software engineering, companion proceedings (ICSE-companion). IEEE; 2021. p. 17–20.
8. Shi L, Wang Z, Zeng Y. Edge network security risk control based on attack and defense map. J Circuits Syst Comput. 2021;30(03):2150046.
9. Kwon J, Buchman E. Cosmos whitepaper. A Netw. Distrib, Ledgers: 27. 2019.
10. Wood G. Vision for a heterogeneous multi-chain framework. White Pap. 2016;21(2327):4662.
11. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. IEEE; 1994. p. 124–34.
12. Grover LK. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett. 1997;79(2):325.
13. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J Comput. 1997;26(5):1484–509.
14. Lee Y, Son B, Jang H, et al. Atomic cross-chain settlement model for central banks digital currency. Inf Sci. 2021;580:838–56.
15. Zamyatin A, Harz D, Lind J, et al. Xclaim: trustless, interoperable, cryptocurrency-backed assets. In: 2019 IEEE symposium on security and privacy (SP). IEEE; 2019. p. 193–210.
16. Cui Y. A cross-chain protocol based on quantum teleportation for underlying architecture of metaverse. In: 2022 7th International Conference on Computer and Communication Systems (ICCCS). IEEE; 2022. p. 508–12.
17. Yiting F, Zhaofeng M, Danheng X, Pengfei D. Security strength assessment method of blockchain entered across links. Inf Netw Secur. 2023;23(01):84–92.
18. Qu Z, Li Y, Sun L, Yu Y, Muhammad G. SCS-QBCT: a Supply Chain System-Driven Efficient Quantum Blockchain Cross-Chain Transaction Scheme. IEEE Internet Things J. 2025.
19. Yu H, Huang M. Anti-quantum cross-chain identity authentication approach using dynamic group signature. Front Inf Technol Electron Eng. 2025;26(5):742–52.
20. Zhang S, Zhou R, Wang L, Xu S, Shao W. Cross-chain asset transaction method based on ring signature for identity privacy protection. Electronics. 2023;12(24):5010.
21. Li C, Jiang B, Dong M, Chen Y, Huang M, Xin X, Ota K. Cross-Chain Privacy-Preserving for BIoMT with Designated Verifier Proxy Signature. IEEE Internet Things J. 2025.
22. Cui W, Dou T, Yan S. Threats and opportunities: blockchain meets quantum computation. In: 2020 39th Chinese Control Conference (CCC); 2020. p. 5822–4.
23. Xin X, Ding L, Li C, et al. Quantum public-key designated verifier signature. Quantum Inf Process. 2022;21(1):33.
24. Huang Y, Xu G, Song X. An improved efficient identity-based quantum signature scheme. Quantum Inf Process. 2022;22(1).
25. Xin X, Zhang T, Yang Q, Li C. Quantum signature based on multi-arbitrators and product states. Mod Phys Lett B. 2022;36(28n29).
26. Ye F, Zhou Z, Li Y. Quantum-assisted blockchain for IoT based on quantum signature. Quantum Inf Process. 2022;21(9).
27. Wang Z, Li J, Chen X, Li C. A secure cross-chain transaction model based on quantum multi-signature. Quantum Inf Process. 2022;21(8).
28. Chen HM, Jia HY, Wu X, et al. Public-key quantum signature for classical messages without third-party verification. Quantum Inf Process. 2022;21(8).

29. Xin X, Ding L, Yang Q, Li C, Zhang T, Sang Y. Efficient chain-encryption-based quantum signature scheme with semi-trusted arbitrator. Quantum Inf Process. 2022;21(7).
30. Miller F. Telegraphic code to insure privacy and secrecy in the transmission of telegrams. CM Cornwell. 1882.
31. Bellovin SM. Frank Miller: inventor of the one-time pad. Cryptologia. 2011;35(3):203–22.
32. Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J. 1949;28(4):656–715.
33. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.
34. Huang XJ, Li ZZ, Li ZC. Quantum Signature Scheme Based on Secret Sharing. Int J Theor Phys. 2022;61(6).
35. Chen M, Xin X, Chen D. Quantum Signature without Classical Private Key. Int J Theor Phys. 2022;61(2).
36. Lu D, Li Z, Yu J, Han Z. A Verifiable Arbitrated Quantum Signature Scheme Based on Controlled Quantum Teleportation. Entropy. 2022;24(1).
37. Gottesman D, Chuang I. Quantum digital signatures. 2001. arXiv:quant-ph/0105032.
38. Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps. 2003 lecture notes in computer science. Berlin: Springer; 2003. p. 416–32.
39. Yang L, Xiang C, Li B. Quantum probabilistic encryption scheme based on conjugate coding. China Commun. 2013;10(2):19–26.
40. Yang L, Yang B, Pan J. Quantum public-key encryption protocols with information-theoretic security. In: New York proceedings of SPIE-the international society for optical engineering. IEEE; 2010. p. 8440.
41. Feng Y, Ying M. Quantum Hoare logic with classical variables. ACM Trans Quantum Comput. 2021;2(4):1–43.

Publisher's note