



Article

Cross-Chain Asset Transaction Method Based on Ring Signature for Identity Privacy Protection

Shuhui Zhang ^{1,2,*} , Ruiyao Zhou ^{1,2}, Lianhai Wang ^{1,2} , Shujiang Xu ^{1,2} and Wei Shao ^{1,2}

¹ Key Laboratory of Computing Power Network and Information Security, Ministry of Education, Shandong Computer Science Center (National Supercomputer Center in Jinan), Qilu University of Technology (Shandong Academy of Sciences), Jinan 250353, China; 10431210369@stu.qilu.edu.cn (R.Z.); wanglh@sdas.org (L.W.); xushj@sdas.org (S.X.); shaow@sdas.org (W.S.)

² Shandong Provincial Key Laboratory of Computer Networks, Shandong Fundamental Research Center for Computer Science, Jinan 250014, China

* Correspondence: zhangshh@sdas.org

Abstract: In recent years, the rapid development of blockchain technology has facilitated the transfer of value and asset exchange between different blockchains. However, achieving interoperability among various blockchains necessitates the exploration of cross-chain technology. While cross-chain technology enables asset flow between different blockchains, it also introduces the risk of identity privacy leakage, thus posing a significant threat to user security. To tackle this issue, this article proposes a cross-chain privacy protection scheme that leverages ring signature and relay chain technology. Specifically, this scheme utilizes RCROSS contracts based on ring signatures to handle cross-chain transactions, thereby ensuring the privacy of both parties involved in the transaction. This cross-chain solution demonstrates practicality and efficiency in facilitating cross-chain asset trading. Furthermore, it effectively combats reuse attacks and man-in-the-middle attacks at the application layer while also providing resistance against denial-of-service attacks at the network layer. To validate the proposed cross-chain solution, we conducted tests by constructing a specific cross-chain scenario and by focusing on the natural gas consumption values generated by the RCROSS contract function used in the application chain. The findings indicate that our proposed solution is highly practical in safeguarding the identity privacy of transaction participants. This article's framework guarantees reliability, security, and efficiency in cross-chain asset transactions. By incorporating ring-based signatures and relay chain technology, users can confidently protect their identity privacy, thus ensuring secure and smooth cross-chain transactions.

Keywords: cross-chain asset transaction; ring signature; identity privacy protection



Citation: 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*, 5010. <https://doi.org/10.3390/electronics12245010>

Academic Editor: Zbigniew Kotulski

Received: 3 November 2023

Revised: 9 December 2023

Accepted: 11 December 2023

Published: 14 December 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the continuous evolution of blockchain technology, a multitude of blockchain systems have emerged and are in the process of development. Yet, this rapid growth presents a significant challenge known as the “island” problem, which hinders seamless value transfer and information interaction between distinct blockchains. Consequently, enabling the realization of value transfers and information integration across different blockchain networks has become a prominent area of research within the blockchain field. One of the key solutions to this challenge is cross-chain technology, which aims to address the interoperability problem between diverse blockchain platforms. However, while cross-chain technology holds promise, it is important to recognize that most existing implementations suffer from privacy vulnerabilities. Protecting cross-chain data and identities becomes crucial when interacting with different blockchains. Given the substantial differences between various chains, the cross-chain operation remains particularly susceptible to privacy breaches. Attackers can exploit weaknesses by eavesdropping on nodes and intercepting cross-chain data, thereby compromising sensitive private information. Consequently, privacy concerns

during the cross-chain process persist, resulting in potential privacy leakage. Overall, ensuring a secure and private cross-chain environment necessitates robust measures to safeguard data and identities throughout the process. Addressing these concerns is pivotal for advancing the adoption and progress of cross-chain technology.

The existing cross-chain mechanisms include notary public mechanisms, relay, and hash-locking, but all of these cross-chain mechanisms pose a risk of privacy leakage. The notary mechanism includes a single-signature notary mechanism and a multisignature notary scheme. The single-signature notary mechanism carries the risk of a single point of failure [1]. Although the multisignature notary human-machine system weakens the centralization risk, there is still a risk of collusion between notary nodes; thus, there is a risk of leakage of user identity privacy and transaction privacy [2]. In the relay model, the implementation of cross-chains based on relays also needs to avoid the privacy leakage risk caused by the malicious behavior of relay nodes [3]. In the hash-locking model, people pay more attention to the fairness of atomic exchange, thus ensuring that both parties' assets are exchanged or not exchanged, and the user's identity privacy and transaction privacy are not effectively protected. At the same time, the hash-locking scheme is only applied in homogeneous cross-chain scenarios and does not have compatibility [4]. It can be observed that different cross-chain methods all carry the risk of privacy leakage. Privacy protection can be categorized into two main aspects: transaction privacy and identity privacy. Identity privacy leakage refers to the issue where users' identities are not adequately protected due to the blockchain's open and transparent nature; thus, this has become a significant concern. Identity privacy holds great importance in blockchains, and, initially, transaction pseudonymization could achieve a certain level of anonymity. However, with the continuous development of tracking technology and the statistical analysis of open transaction data, the topology of all transaction data can be constructed. Via this topology, the relationship between transaction participants and their real information can be analyzed to a certain degree. Consequently, relying solely on traditional pseudonyms becomes challenging relative to guaranteeing identity privacy in transactions.

Identity privacy in cross-chain scenarios refers to the safeguarding of the connection between the sender and the source chain address, as well as the connection between the recipient and the destination chain address. Lately, numerous attacks have targeted cross-chain transactions. For instance, in July 2021, AnySwap, a cross-chain project, experienced a hack due to the theft of the administrator's private key, leading to losses exceeding USD 8 million. Additionally, in August 2021, Poly Network, an interoperability protocol for cross-chain transactions, encountered a hack resulting in losses surpassing USD 600 million. These incidents highlight the urgent need for enhanced cross-chain security and the prevention of privacy breaches concerning transaction senders and receivers.

Building upon the aforementioned background analysis, we propose a cross-chain asset transaction scheme centered on ring signatures to address the lack of user identity privacy protection in current cross-chain transactions. The key contributions of this paper are as follows:

- (1) Given the present vulnerability of user identity privacy in cross-chain asset transactions, we have designed a new scheme that utilizes ring signatures to provide secure and privacy-protecting transactions. This scheme effectively addresses the issue of user identity leakage.
- (2) In order to achieve efficient user management, cross-chain transaction processing, and identity privacy protection, we have developed the RCROSS contract. This contract seamlessly integrates ring signature and cross-chain management, allowing for streamlined operations and enhanced security measures.
- (3) The performance evaluations of appchains accessing the cross-chain network demonstrate the high compatibility and privacy protection achievements of our proposed cross-chain scheme for both homogeneous and heterogeneous chains.

The arrangement of this article is as follows. In the first section, we first summarize the background of cross-chain asset transactions and the privacy leakage issues currently

faced. In the second section, we take the current status of identity privacy protection in single-chain and cross-chain backgrounds as research entry points, summarize the relevant work of researchers in recent years related to identity privacy protection, and, finally, summarize the shortcomings of existing identity privacy protection technologies in cross-chain scenarios. In the third section, we briefly introduce the model architecture of this scheme and propose detailed design objectives. In the fourth section, we further refine the model architecture proposed in the third section and elaborate on the specific solution for implementing identity privacy protection in cross-chain scenarios. In the fifth section, we conduct an experimental evaluation. In order to ensure the high practicality of this scheme, we test the gas consumption required for deploying contracts on the Ethereum platform, and, finally, we analyze the transaction delay caused by users completing a cross-chain transaction. In the sixth section, we discuss security, which corresponds to the security design objectives proposed in the third section. In the seventh section, we first summarize the conclusions drawn from this plan, and, finally, we look forward to our future research plans.

2. Related Work

To safeguard user identity privacy and prevent data analysis of the public ledger, scholars have proposed an enhanced scheme based on the transaction model of mainstream public chains. This involves integrating zero-knowledge proof and trusted execution environment privacy protection technologies to ensure robust identity privacy protection. Additionally, as the demand for privacy increases, anonymous coins like Monroe Coin and Zero Coin are emerging and gaining momentum. Regarding the targeted protection of identity privacy protection technology, these technologies can be categorized into sender identity hiding and receiver identity hiding. Identity-hiding technology can be further classified into cooperative coin mixing technology, global coin mixing technology, and autonomous coin mixing technology.

Cooperative coin mixing technology, also known as collaborative transaction obfuscation, involves the transaction sender enlisting a group of simultaneous transaction users to collectively complete the transaction, thereby achieving the concealment of the transaction's input and output addresses. Currently, cooperative coin mixing technology can be broadly categorized into two types: centralized coin mixing and decentralized coin mixing. Among the centralized coin mixing schemes, Bonneau and Narayanan et al. proposed the MixCoin scheme [5], which achieves the auditability of the mixing process. However, in the MixCoin scheme, the correspondence between input and output addresses is still visible to third-party institutions. Blind signature technology [6] is a digital signature scheme in which the signer is not visible to signature information, and the signature result is not traceable. Gang Xu, Yibo Cao, and others combined blind signature with blockchain logging to ensure the privacy of log information to a large extent [7]. It can be observed that in the decentralized, mixed-coin scheme, the intermediary institution acts as an obfuscator to complete transaction obfuscation, and although the transaction identities are unlinkable to external observers, the intermediary institution can grasp the identity-linking relationship between the sender and the receiver of mixed-coin transactions. Decentralized mixed-coin schemes, on the other hand, take the approach of removing third-party institutions to avoid the risk of privacy leakage. In a decentralized scheme, users who do not trust each other do not need to rely on a third party and are free to cooperate to construct a mixed-coin transaction. CoinJoin [8], first proposed by Maxwell, is currently a typical decentralized mixed-coin party; however, the CoinJoin transaction does not satisfy internal unlinkability. Therefore, the CoinShuffle [9] scheme is inspired by CoinJoin and adds the sorting protocol Dissen [10] to the scheme to ensure anonymity and robustness against active attacks. The CoinShuffle++ scheme [11], the ValueShuffle scheme [12], and the SecureCoin scheme [13] build upon CoinShuffle to enhance the privacy of the P2P mix. Monroe Coin [14] serves as a prime example of autonomous hybrid coin technology. It is an open-source cryptocurrency derived from Bitcoin, and its users can realize autonomous coin mixing without the

participation of a third-party central institution and other users in the coin mixing process, which can effectively eliminate the problems faced by the original coin mixing scheme. The design of Monroe Coin is based on the CryptoNote protocol [15] and provides stronger privacy protection features. In terms of identity privacy, Monroe Coin realizes the identity privacy of both sides of the transaction; the identity of the sender of the transaction is hidden based on the ring signature, and the identity of the receiver of the transaction is hidden based on the one-time address. The combination of disposable address and ring signature constitutes the autonomous coin mixing technology of Monroe Coin. Monroe Coin also continuously optimizes ring signature technology in the development process. In 2015, Back et al. proposed a storage space optimization scheme for CryptoNote's one-time signature results [16], which is based on the linkable self-organizing anonymous group signature technology scheme, LSAG, proposed by Liu et al. [17], but the LSAG scheme also has deficiencies, and it only supports single-input transaction identity obfuscation. Moreover, to a certain extent, the anonymity set is too small in the transaction process. As a result, a subsequent version of the Monroe Coin Ring Secrets transaction proposed the multi-layer connectable self-organizing group anonymity scheme: MLSAG [18]. The most typical representative of global mixed-coin technology is Zero Coin (Zcash) [19], a strong privacy-preserving open-source cryptocurrency initiated by researchers at MIT and Hopkins University. It follows the UTXO transaction structure in Bitcoin and provides stronger privacy-preserving features by introducing Merkle trees, zero-knowledge proofs, and cryptography. In 2013, Miers et al. designed Zero Coin [20], an anonymous, distributed, blockchain-based e-cash system, which guarantees the integrity of the cryptocurrency list via the use of a blockchain. In 2014, Ben-Sasson et al. designed an upgraded version of Zero Coin, Zerocash [21], thus laying the theoretical foundation of the Zcash transaction protocol. Zcash, a cryptocurrency designed based on Zerocash, has been developed with respect to two major versions: Sprout and Sapling. In terms of identity privacy, Zero Coin realizes the identity concealment of the transaction sender based on the global mixing of coins and zero-knowledge proofs and the identity concealment of the transaction receiver via the on-chain encrypted transmission of transaction contents. C Lin and D He et al. [22] designed a DCAP conditional anonymous payment system, which was compared with Zerocash in the same testing environment and showed high practicality.

Based on the analysis of research related to identity privacy protection in single-chain scenarios, we can consider introducing global and autonomous coin mixing technologies into cross-chain asset transactions. Research about identity privacy in cross-chain scenarios has also received increasing attention. Cao et al. [23] proposed an asset swap anonymization scheme based on zero-knowledge proof and hash-locking techniques to protect both parties' transaction privacy during cross-chain asset transactions. However, its solution suffers from limitations in application scenarios and low cross-chain efficiency. Li et al. also designed ZeroCross based on zero-knowledge proof [24], a privacy-preserving cryptocurrency for Monroe Coin exchange solutions. The scheme also utilizes zero-knowledge proofs to resist remote side-channel attacks in cross-chain asset exchanges, and it is proved in the UC framework for ZeroCross. The Zendoo protocol is proposed by Garoffolo et al. in order to construct a decentralized and verifiable cross-chain asset transfer protocol based on the sidechain and zk-SNARK protocols; this was carried out to achieve a bi-directional transfer operation of assets between the mainchain and the sidechain. The Zendoo protocol is based on the sidechain and zk-SNARK protocols. Zendoo's cross-chain transfer protocol connects the mainchain to all sidechains derived from the mainchain; it allows for sending currencies to sidechains and receiving them safely and securely, and it is a two-way protocol that defines two basic operations: forward transfer (FT, forward transfer) and backward transfer (BT, backward transfer). Zk-SNARK provides proof of ownership of certain information without disclosing it, and Zendoo implements effective transfer verification based on zk-SNARK for the main chain. In addition to solving the problem of privacy protection in cross-chain scenarios based on zero-knowledge proofs, there are also implementations based on signature algorithms. However, introducing zero-knowledge proof technology

into cross-chain scenarios has some drawbacks. Firstly, the privacy protection mechanism based on zero-knowledge proof requires the generation of a public–private key pair as a system parameter before all transactions occur. This system parameter generation process is not consensus based, and the current mainstream approach is to generate it through blockchain development teams, which introduces security risks. If the development team wants to do evil, it will harm the interests of the users. Secondly, the privacy protection mechanism based on zero-knowledge proof exhibits high operational complexity not only in terms of time but also in terms of spatial complexity. In summary, privacy protection mechanisms based on zero-knowledge proof require a trusted third party to generate system parameters, which is costly to run and inefficient.

Based on the above analysis of cross-chain privacy protection schemes, it can be concluded that currently proposed cross-chain privacy protection schemes have certain drawbacks, most schemes are designed for the privacy leakage of transaction contents, and research related to identity privacy protection is still in a blank state. Considering the inherent difficulty of implementing cross-chain technology, efforts should be made to enhance identity privacy protection.

3. System Overview

3.1. System Model and Roles

The cross-chain privacy protection scheme utilizing ring signatures is presented in Figure 1 and implemented on the Ether and Fabric federation chains. This system facilitates secure transfer transactions between the source chain, where the transaction sender is located, and the blockchain, where the transaction receiver is situated. Additionally, the system classifies participants to ensure the seamless execution of transfer transactions:

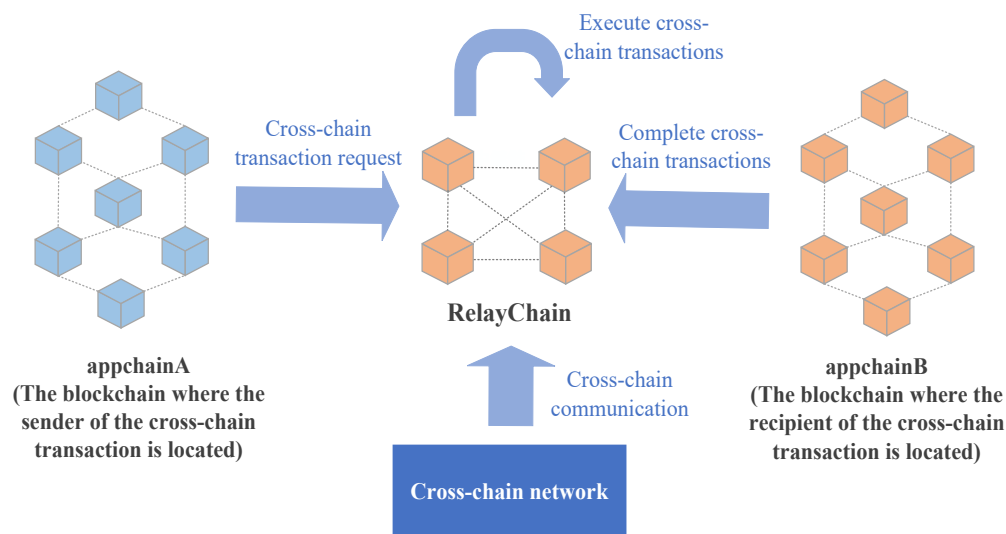


Figure 1. Overall scheme architecture diagram.

Users: Users are categorized into two groups: transaction senders and transaction receivers. Transaction senders initiate cross-chain transaction requests on their appchain, thus triggering a transfer process. Meanwhile, transaction receivers receive the equivalent amount of assets in their appchain account, which matches the transferred amount.

Appchain: The appchain refers to the blockchain where the user carrying out the cross-chain transaction is situated. Herein, this paper assumes that the appchain has a high level of security, and any non-cross-chain asset transactions executed on this blockchain are highly credible.

Cross-chain network: The cross-chain network facilitates the handling of cross-chain events generated by the appchain. Through this network, transaction requests can be sent to the destination address of the respective appchain. The relay chain and gateway within the cross-chain network process transaction requests that require transmission. The relay

chain is responsible for processing cross-chain asset transactions. It verifies the transaction signature, ensures the legitimacy of the signature, and further verifies the validity and existence of the transaction upon passing these checks. Finally, it categorizes the transaction based on the destination address and sends it to the corresponding gateway. The gateway, on the other hand, is capable of listening to transaction events initiated by the appchain. It places the transaction in the pending transaction pool after receiving the transaction event.

3.2. Design Goal

With the rapid implementation of numerous blockchain projects, promoting cross-industry collaborations and resolving interoperability challenges among diverse blockchain architectures and business models have emerged as a prominent focus of current blockchain research. Specifically, within the financial sector, there is a pressing need to develop secure and dependable cross-chain asset transaction schemes. However, due to the comparatively recent emergence of cross-chain technology and the associated risks involved, there exist several technical challenges in researching cross-chain asset transaction methods.

- (1) **Limited application scenarios:** Many cross-chain research proposals mainly focus on asset transactions between similar chains. Although some breakthroughs have been made in enabling cross-chain asset transactions between different chains, they are mostly limited to public chain, public chain or alliance chain, and alliance chain transactions. These limitations arise from challenges inherent in cross-chain technology, including difficulties in achieving interoperability across underlying architectures, aligning with business models, and establishing mutual trust in security mechanisms. As a result, conducting cross-chain asset transactions between public chains and alliance chains has proven to be increasingly challenging. To overcome these obstacles, it is necessary to design a cross-chain asset transaction scheme that is not restricted by chain types, which would facilitate greater flexibility and applicability.
- (2) **Cross-chain security issues:** Cross-chain technology itself has a certain fragility, and special attention needs to be paid to ensuring the security of transactions in cross-chain scenarios. Currently, most proposed cross-chain asset-trading schemes consider the harm caused by network-layer attacks, demonstrating their superiority in resisting denial-of-service attacks and reuse attacks. However, there is relatively little consideration given to attacks against application-layer user accounts. In the scenario of cross-chain asset trading, it is necessary to ensure that there is no risk of data leakage or interception by third parties. At the same time, it is necessary to consider network- and application-layer attacks. Among them, attacks targeting user accounts in application-layer attacks cause the greatest harm to transactions. Therefore, it is necessary to consider both network-layer security and application-layer security to ensure the security of cross-chain asset trading.
- (3) **Cross-chain identity privacy leakage:** Due to the unique decentralization and other characteristics of the blockchain itself, blockchain and cross-chain technology have the characteristics of openness and transparency, but, for most users, excessive openness and transparency will threaten their privacy and security; thus, it is necessary to design a cross-chain method to protect the user's identity and privacy.
- (4) **Cross-chain transaction performance issues:** With the continuous expansion of cross-chain transaction scales, the performance demand of cross-chain transactions on concurrent execution speeds is increasing, which results in a gradual increase in cross-chain technology requirements with respect to transaction-processing performance; thus, it is necessary to design a secure cross-chain asset transaction scheme that refrains from imparting large impacts on transaction-processing performances.

Therefore, regarding the technical challenges identified in research related to cross-chain asset transaction methods, this paper proposes design objectives from three perspectives: scheme design, security assurance, and transaction performance.

- (1) Scheme design: It is necessary to design an achievable plan that enables cross-chain asset transactions between heterogeneous chains, overcomes the challenges of application scenario restrictions, and achieves plug-and-play compatibility for the appchain in cross-chain asset transactions.
- (2) Security: In addition to the attacks easily suffered by the network layer, it is also necessary to take into account the attacks launched against the account faced by the application layer. Based on the above security issues, a cross-chain solution is designed to protect the security of the user account and to realize the defense against the security attacks that may be faced in the cross-chain asset transactions.
- (3) Privacy protection: In addition to the attacks that the network layer is susceptible to, it is also necessary to consider the attacks launched against accounts by the application layer. Based on the above security issues, a cross-chain solution is designed to protect the security of user accounts, which provides defenses against potential security attacks in cross-chain asset transactions.
- (4) Transaction performance: Compared with existing relay cross-chain asset-trading schemes, the impact on the performance of relay cross-chain schemes will be controlled within an acceptable range for users, thus fully guaranteeing the practicality of the scheme.

3.3. Preliminary Knowledge

Cross-chain asset transaction: Cross-chain asset transaction is a crucial aspect of cross-chain technology, as it enables the secure and reliable transfer of data or information from one blockchain system to another. The ultimate goal of researching cross-chain technology is to achieve value transfer and data interoperability between different blockchain systems. Cross-chain asset transaction, which mainly consists of cross-chain asset transfer and cross-chain asset exchange, is the means of realizing value transfer between different blockchains. Cross-chain asset exchange, also known as atomic exchange, is a cross-chain transaction that has atomicity and consistency and essentially involves the flow of assets among the respective blockchains. Cross-chain asset transfer supports the transfer of assets between different chains, which also has atomicity and decentralized consistency. It essentially involves the freezing (destruction) of assets on one blockchain and the unfreezing (creation) of assets on another blockchain.

Ring signature: The concept of the ring signature is a type of digital signature proposed by Rivest, Shamir, and Tauman in 2001. In the process of generating a ring signature, the actual signer selects a group of members (including themselves) as potential signers and signs the message using their private key and the public keys of other group members. The selected group of members is known as the ring, and the resulting signature is referred to as the ring signature. While others can verify the validity of the signature using the public key of the member and the ring signature, they cannot ascertain the specific member who is responsible for the signature.

Let the real signer be ID_u ; the ring used to generate the ring signature is $R = \{ID_u | i = 1, 2, \dots, n\}$. Then, the generated verifiable ring signature σ needs to meet the following properties:

Property 1 (unforgeability): For a correct and valid signature σ , an attacker cannot generate a fake signature on a message m that passes verification without access to the private key of any member of the ring.

Property 2 (anonymity): The probability that an attacker can deduce the identity of the true signer from the signature is $1/r$ (r is the number of ring members in the signature ring R).

Property 3 (uniqueness): The uniqueness property intuitively means that a set of colluding signers in a ring cannot produce signatures for any messages with more unique identifiers than the size of the set.

4. Specific Scheme

4.1. Scheme Framework

This section primarily focuses on the process of transferring and declaring assets from appchainA to appchainB. To illustrate this, we consider two different highly secure blockchain systems. In this scenario, a user on appchainA intends to send a transfer transaction to a user on appchainB. Even though these two blockchain systems may lack interoperability, they possess a high degree of trustworthiness. In this paper, we propose a cross-chain asset transaction method that ensures user identity privacy by leveraging the solid design of the two trustworthy blockchain systems. The solution utilizes relay chain cross-chain technology and introduces ring signature technology to protect the transaction initiator's identity privacy. The specific framework flow of this method is presented in Figure 2.

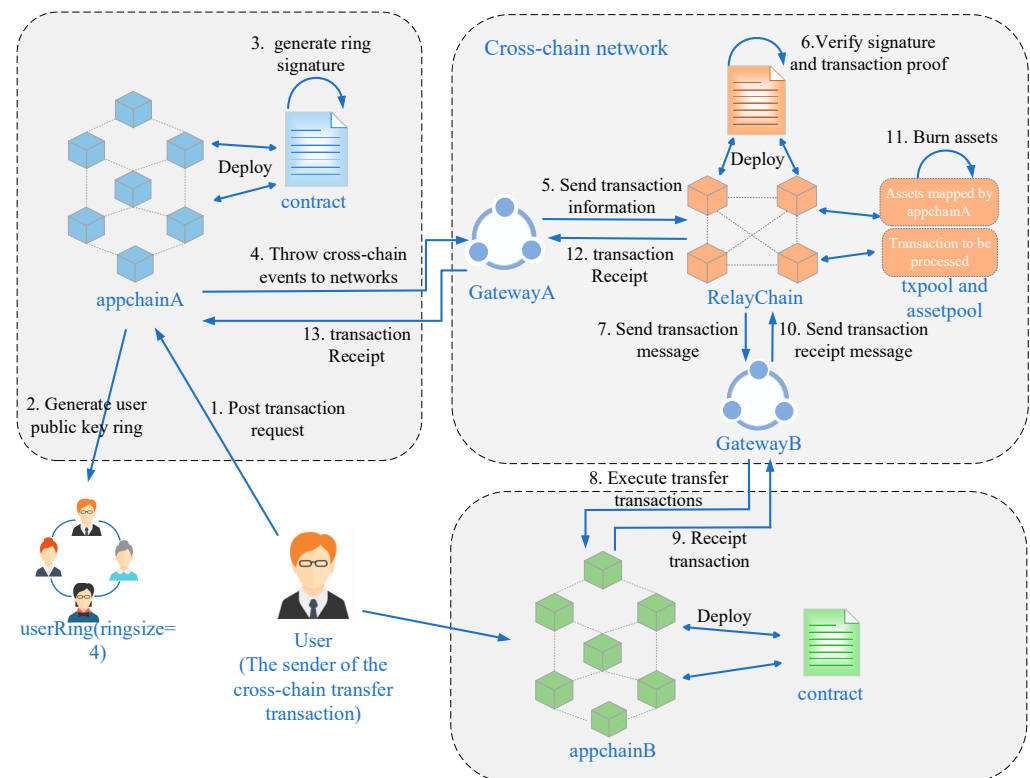


Figure 2. Scheme-specific framework diagram.

A sender user on appchainA initiates a transfer transaction to a receiver user on appchainB, which consists of the following:

- (1) Initialize: To initiate a transaction, the user must first ensure that their account has sufficient assets and deploy the RCROSS contract to the appchain. Upon successful deployment, the corresponding contract address will be returned. Following this, the user must register the information of both appchainA and appchainB in the relay chain, including the appchain type, RCROSS contract address, and address information for the subsequent verification of appchain transaction information. The user needs to register validation rules in the relay chain to facilitate its validation of appchain transaction information. Finally, the user should call the Ringsign() algorithm to generate the corresponding user ring based on the transaction initiator's public key information, which is then packaged into the cross-chain transaction's information.
- (2) Publish transaction request: In the transaction request publishing process, the transaction initiator on appchainA initiates a cross-chain transaction. At this stage, the status of the cross-chain transaction is set to START. The cross-chain transaction's information includes various details, such as the public key user's ring, random

- number, number of transfers, addresses of appchainA, appchainB, and the relay chain, and the current status of the transaction's information. The transaction initiator then broadcasts this transaction request relative to the network of appchainA.
- (3) Transaction request delivery: This step is divided into two main parts. The first part involves forwarding the request from the appchain to the cross-chain network during the transaction delivery stage. The second part involves forwarding the request from the cross-chain network to the appchain. The types of requests include cross-chain transaction requests and cross-chain transaction request acknowledgment. In the first part, sending the request from the appchain to the cross-chain network occurs when the SDK calls the RCROSS contract to trigger the cross-chain event. The gateway in the cross-chain network listens to this event, extracts the relay chain address information from the cross-chain transaction details, and forwards the cross-chain event to the transaction pool controlled by the corresponding relay chain address. In the second part, sending the request from the cross-chain network to the appchain happens when the gateway receives transaction information sent by the relay chain. The gateway then parses the transaction's details and forwards the request to the appchain. Similarly, when the gateway receives transaction information sent by the relay chain, it parses the information and broadcasts the cross-chain event to the appchain that was obtained via parsing.
 - (4) Transaction processing via the relay chain: Transaction processing via the relay chain mainly consists of two parts. The first part comprises the verification of cross-chain transaction information during the transaction's sending phase, and the second part comprises the resolution of cross-chain transaction statuses via the relay chain during the transaction's acknowledgment phase. During the transaction's sending phase, the relay chain retrieves the pending transaction request from the transaction pool and processes it. The relay chain verifies the issued cross-chain transaction's information. It extracts the random number and the initiator's user public key ring signature from the cross-chain transaction information. Separately, it verifies the random number and the ring signature by using the VerifySign() function to check their correctness and legitimacy. After the verification process, it applies the mapping function to validate the ring signature's legitimacy and maps the digital asset in appchainA to the address controlled by the relay chain. Once the verification is successfully passed, transaction information is then routed to the gateway. Moving on to the transaction acknowledgment stage, the relay chain obtains the transaction status from the transaction acknowledgment information. If the transaction status is SUCCESS, the relay chain destroys the assets of the corresponding user in the address controlled by the relay chain. Conversely, if the transaction status is FAIL, the relay chain sends the assets from the address controlled by the relay chain back to the user who initiated the transaction.
 - (5) AppchainB executes the transaction: Upon receiving the cross-chain transaction request from the cross-chain network, appchainB executes the transfer transaction, thus allowing the user to receive the corresponding amount of digital assets. Once the transaction is executed, appchainB updates the transaction status and sends the cross-chain transaction acknowledgment to the cross-chain network. This enables the transaction request to be transmitted back to the relay chain.

4.2. Ring Signature Algorithm

This section provides an introduction to the ring signature algorithm utilized in this scheme. In terms of choosing the appropriate algorithm, we carefully considered the computational limitations of smart contracts and opted for a lightweight hash algorithm. Specifically, the unique ring signatures proposed by Matthew Franklin [25] are employed, with SHA-256 serving as the hash algorithm for generating and verifying ring signatures. SHA-256 strikes a favorable balance between security and performance, thereby offering enhanced efficiency.

Additionally, we have optimized the parameters of the ring signature algorithm to enhance compatibility within this scheme and to create a more lightweight ring signature algorithm. Primarily, we achieved this by reducing the number of ring members, thereby effectively streamlining the processing of ring signatures. It is worth noting that the ring signature algorithm still maintains a high level of flexibility, thus enabling users to adjust the ring size based on their privacy requirements. For users with higher security standards, increasing the number of ring members strengthens privacy protection. Conversely, users seeking to maintain a lightweight ring signature algorithm while ensuring security can opt to reduce the number of ring members.

When a user initiates a transaction request, the first step involves the initialization and generation of user keys. Following this, the ring signature is computed using the generative ring signature algorithm. In the transaction phase, the relay chain utilizes the ring signature verification algorithm to process and verify the ring's signature.

4.2.1. Ring Signature Algorithm

This ring signature method mainly consists of four parts: initialization algorithm $\text{Setup}(1^\lambda)$, user key generation algorithm $\text{RG}(1^\lambda, \text{pp})$, generating ring signature algorithm $\text{RS}(\text{sk}_i, R, m)$, and verifying ring signature algorithm $\text{RV}(R, m, \sigma)$.

Initialization algorithm $\text{Setup}(1^\lambda)$: First, a generic random string $\eta \leftarrow \{0, 1\}^{l(\lambda)}$ is chosen with a pseudo-random function mapping: $F : S \times X \rightarrow Y$, where S is the key, X is the message, Y is the range, CM is a character commitment scheme, and Com is a commit algorithm that outputs the public parameters as

$$\text{pp} = (\lambda, \eta, F, \text{CM})$$

Key generation algorithm $\text{RG}(1^\lambda, \text{pp})$: The key of the user generation algorithm takes parameter s_A as the input, which is based on the randomly selected computational string commitment C_A , and outputs public key $\text{pk}_A = (\text{pp}, C_A)$ and private key $\text{sk}_A = (\text{pp}, s_A, r_A)$.

Generating ring signature algorithm $\text{RS}(\text{sk}_i, R, m)$: A message m is signed in the ring $R = (\text{pk}_A, \text{pk}_1, \dots, \text{pk}_{n-1})$, and the signer generates a signature using their private key sk_A , which is denoted as follows:

$$(R, m, \sigma)$$

where $\sigma = (\tau, \pi)$ and π is a publicly verifiable, non-interactive, zero-knowledge proof $(\{C_j\}_{j=1}^n, R, m, \tau) \in L_{\text{OR}}$, where $L_{\text{OR}} := \{(\{C_j\}_{j=1}^n, R, m, \tau) | \exists (j, s_j, r_j)[C_j = \text{Com}(s_j, r_j) \text{ and } \tau = F_{s_j}(M || R)]\}$.

Verification ring signature algorithm $\text{RV}(R, m, \sigma)$: The algorithm first resolves σ relative to (τ, π) and checks if π is a correct noninteractive zero-knowledge proof for L_{OR} .

4.2.2. Three Characteristics of the Ring Signature

Next, we will demonstrate the feasibility of the ring signature from three characteristics: unforgeability, anonymity, and uniqueness. We firstly establish several concepts. If x is a string, then $|x|$ denotes its length. If S is a set, then $|S|$ denotes its size and $s \xleftarrow{\$} S$ denotes the operation of selecting an element s of S uniformly at random. \emptyset denotes the empty set, while $\emptyset\emptyset$ denotes a vector of empty sets. If \mathcal{A} is a randomized algorithm, then we write to indicate the operation that runs \mathcal{A} on inputs x, y, \dots and a uniformly selected r from an appropriately required domain and outputs z . We write $z \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_1, \mathcal{O}_2, \dots}(x, y, \dots)$ to indicate the operation that runs \mathcal{A} with access to oracles $\mathcal{O}_1, \mathcal{O}_2, \dots$ on inputs x, y, \dots and outputs z .

Unforgeability: In ring signature $RS = (RK, RS, RV)$, we assume the presence of an attacker \mathcal{A} and conduct the following experiments against that attacker:

Experiment $\text{Exp}_{RS,n}^{\text{uf}}(\mathcal{A})$
 $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \text{RK}(1^\lambda); \text{CU} \leftarrow \emptyset; \text{RS}_{R,M} \leftarrow \emptyset \emptyset$ where $T \leftarrow \{pk_i\}_1^n$
 $(i_0, i_1, R, m) \xleftarrow{\$} \mathcal{A}^{\text{USK}(\cdot), \text{RS}(\cdot, \cdot, \cdot)}(T)$
 $b \xleftarrow{\$} \{0, 1\}; \sigma \xleftarrow{\$} \text{RS}(sk_{i_b}, R, m)$
 $b' \xleftarrow{\$} \mathcal{A}^{\text{USK}(\cdot), \text{RS}(\cdot, \cdot, \cdot)}(T)$
 if $RV(R, m, \sigma) = 0$ then return 0

Here, it is required that $R \subseteq T \setminus \text{CU}$ and \mathcal{A} never queried $\text{RS}(\cdot, \cdot, \cdot)$ with (\cdot, R, m) . We define the advantage of \mathcal{A} in the above experiment as follows:

$$\text{Adv}_{RS,n}^{\text{uf}}(\mathcal{A}) = \Pr[\text{Exp}_{RS,n}^{\text{uf}}(\mathcal{A}) = 1].$$

Based on the above assumptions, we can conclude that the ring signature satisfies unforgeability.

Anonymity: In ring signature $RS = (RK, RS, RV)$, we assume the presence of an attacker \mathcal{A} and conduct the following experiments against that attacker:

Experiment $\text{Exp}_{RS,n}^{\text{anon}}(\mathcal{A})$
 $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \text{RK}(1^\lambda); \text{CU} \leftarrow \emptyset; \text{RS}_{R,M} \leftarrow \emptyset \emptyset$ where $T \leftarrow \{pk_i\}_1^n$
 $(i_0, i_1, R, m) \xleftarrow{\$} \mathcal{A}^{\text{USK}(\cdot), \text{RS}(\cdot, \cdot, \cdot)}(T)$
 $b \xleftarrow{\$} \{0, 1\}; \sigma \xleftarrow{\$} \text{RS}(sk_{i_b}, R, m)$
 $b' \xleftarrow{\$} \mathcal{A}^{\text{USK}(\cdot), \text{RS}(\cdot, \cdot, \cdot)}(\text{guess}, \sigma, s)$
 if $b' \neq b$ then return 0
 return 1

Here, it is mandated that for each $d \in \{0, 1\}$, we have $i_d \notin \text{CU}$ and $i_d \notin \text{RS}_{R,M}$. It may be required that $R \subseteq T$, but this is optional. We define the advantage of \mathcal{A} in the above experiment as follows:

$$\text{Adv}_{RS,n}^{\text{anon}}(\mathcal{A}) = \Pr[\text{Exp}_{RS,n}^{\text{anon}}(\mathcal{A}) = 1] - 1/2.$$

Based on the above assumptions, we can conclude that the ring signature satisfies anonymity.

Uniqueness: In ring signature $RS = (RK, RS, RV)$, we assume the presence of an attacker \mathcal{A} and conduct the following experiments against that attacker:

Experiment $\text{Exp}_{RS,n}^{\text{anon}}(\mathcal{A})$
 $\{(pk_i, sk_i)\}_1^n \xleftarrow{\$} \text{RK}(1^\lambda); \text{CU} \leftarrow \emptyset; \text{RS}_{R,M} \leftarrow \emptyset \emptyset$ where $T \leftarrow \{pk_i\}_1^n$
 $(m, \sigma_1, \dots, \sigma_{|\text{CU} \cup \text{RS}_{T,m}|+1}) \xleftarrow{\$} \mathcal{A}^{\text{USK}(\cdot), \text{RS}(\cdot, \cdot, \cdot)}(T)$
 for $i \leftarrow 1$ to $|\text{CU} \cup \text{RS}_{T,m}| + 1$ do
 if $i \neq j$ then $\gamma_i = \gamma_j$ then return 0
 return 1

Here, each σ_i is of the form $\gamma_i = \gamma_j$. We define the advantage of \mathcal{A} in the above experiment as follows:

$$\text{Adv}_{RS,n}^{\text{unique}}(\mathcal{A}) = \Pr[\text{Exp}_{RS,n}^{\text{unique}}(\mathcal{A}) = 1]$$

In the above experiment, the attacker expected to output multiple signatures, but based on the above assumptions, we can conclude that the ring signature satisfies uniqueness.

4.3. RCROSS Contract

In this paper, a cross-chain contract is designed to achieve identity privacy protection using the ring signature algorithm. The RCROSS contract consists of three main modules: the transaction-information-processing module, the identity privacy protection module, and the cross-chain event-processing module. Deploying the RCROSS contract on the appchain enables the timely processing of cross-chain transaction requests while ensuring privacy protection relative to personal account information. The design framework of the RCROSS contract is depicted in Figure 3.

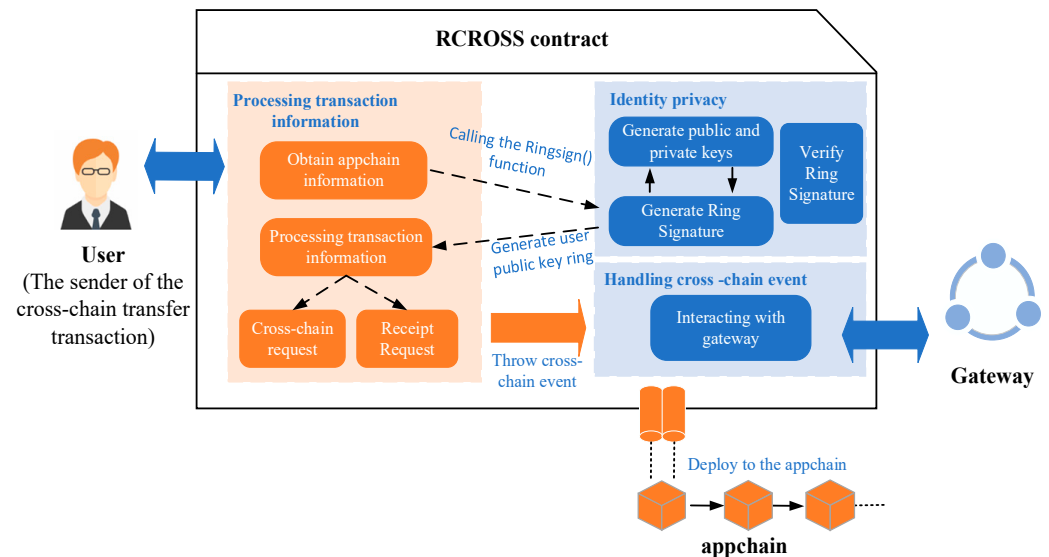


Figure 3. RCROSS contract framework diagram.

To initiate cross-chain asset transactions, users must deploy the RCROSS contract on the appchain. The RCROSS contract allows for the transmission of transaction information between the appchain and the cross-chain network while ensuring the protection of the user's identity information. Within the RCROSS contract, the transaction-information-processing module generates a ring signature by calling the key generation and ring signature generation algorithms of the identity privacy module. The generated ring signature is then returned to the transaction-information-processing module, which re-encapsulates the transaction information and sends it to the cross-chain event-processing module. The cross-chain event-processing module is responsible for interacting with the gateway in the cross-chain network to transmit the transaction information to the relay chain, thus safely transmitting the transaction information in the cross-chain network. Overall, the RCROSS contract guards the privacy of the user's identity on the appchain and enables the processing of cross-chain asset transaction requests by parsing the user's transaction request information, generating a ring signature, and encapsulating it with the original transaction request before interacting with the cross-chain network.

5. Performance

5.1. Experimental Environment Configuration

In the experiment, we utilized Ether and Hyperledger Fabric as the experimental platforms to enable transfer transactions initiated by Ether to Fabric. The Ether smart contract was developed using the Solidity language, while the Fabric chain code was implemented in Golang. The configuration details of the experimental environment are illustrated in Table 1.

Table 1. Environment configuration table.

Environment	Configuration
CPU	AMD Ryzen 7 5800H
Random access memory (RAM)	16 G
GPU	NVIDIA GeForce RTX 3060
System	Ubuntu 20. 04 LTS

5.2. Experimental Environment Configuration

The transaction's processing performance and scalability of blockchain have always been crucial aspects of advancing blockchain technology. When it comes to reaching consensus in a blockchain system, there exists a challenging trade-off among decentralization, security, and scalability. Traditionally, the blockchain system could only prioritize two out of the three. In light of this, the core design concept of this paper is to incorporate ring signatures into cross-chain technology, thereby addressing the issue of user identity privacy leakage in cross-chain asset transactions. The proposed scheme achieves this by obfuscating the ring signature via the utilization of smart contracts on the blockchain, thereby effectively concealing the user's public key information.

In this paper, we compare the ring signature cross-chain method with existing cross-chain methods in terms of performance.

In terms of decentralization, the notary public method is the most centralized. The proposed solution in this article establishes multiple relay nodes and transfers assets through a relay chain consisting of these nodes, thereby improving decentralization compared to the XCLAIM scheme's single relay node setup.

Regarding no claim without burn, the proposed scheme in this article, unlike the DeXTT scheme, accompanies asset destruction on the source chain during cross-chain asset transactions. This ensures asset uniqueness and consistency.

In terms of compatibility, the proposed solution in this article enables asset trading not only between homogeneous chains but also between heterogeneous chains. There are no restrictions on the type of application chain. The experiments in this article were conducted using the Ethereum public chain and Fabric consortium chain. This solution overcomes limitations in cross-chain application scenarios, facilitates cross-chain asset trading between heterogeneous chains, and is applicable to various existing blockchain platforms.

Regarding final certainty, compared to the XCLAIM and DeXTT schemes, this scheme records the transaction status in the transaction receipt, thereby ensuring transaction integrity, reliability, and immutability in transaction confirmations.

In terms of anonymity, in addressing the lack of identity privacy protection in other comparative schemes, the proposed scheme introduces the ring signature algorithm into the relay chain cross-chain asset-trading scenario, thus achieving complete user identity anonymity.

We compared our scheme with the current mainstream cross-chain schemes in terms of decentralization, no claim without burn, compatibility, decentralized finality and anonymity, as shown in Table 2. Through these comparisons, it can be concluded that our scheme has all the above features compared to other schemes.

Table 2. Performance analysis table.

Reference	No Claim without Burn	Compatibility	Decentralization	Decentralized Finality	Anonymity
XCLAIM [26]	✓	✓			
DeXTT [27]		✓	✓		
AgentChain [28]	✓	✓	✓	✓	
Burn-to-Claim [29]	✓	✓	✓	✓	
Proposed Scheme	✓	✓	✓	✓	✓

5.3. Evaluation of Gas Consumption

The proposed solution outlined in this article utilizes Ethereum and Fabric to facilitate cross-chain asset trading. Specifically, the application chain where the transaction initiator is located is the Ethereum private chain. Moreover, this article implements an identity privacy solution by deploying the ring signature algorithm as a smart contract on the Ethereum network. As a result, when evaluating the efficiency of cross-chain asset trading, the primary metric to consider is the gas consumption value of the Ethereum smart contract.

5.3.1. Comparison of the Overall Gas Overhead of Scenarios

This article describes experiments conducted on the same Ethereum private chain with an initial size of four members in the ring. The aim is to illustrate that the gas consumption value of this scheme has not increased significantly compared to other schemes while still being highly practical. To demonstrate this, we compared and tested the gas consumption value in different application scenarios. Firstly, in non-cross-chain scenarios, we deployed the smart contract implementing the ring signature to determine the gas consumption value in Ethereum. We then tested the gas consumption value when deploying the cross-chain contract to Ethereum. Finally, we recorded the gas consumption of deploying the RCROSS contract to Ethereum in the proposed solution. A comparison of gas consumption values is presented in Figure 4a.

Initially, we rewrote the ring signature algorithm into smart contract codes and implemented it for asset transactions on a single Ether chain. The deployment of the ring signature smart contract on Ether resulted in a gas consumption value of approximately 930,000. Furthermore, we deployed the required contract for cross-chain relays without the ring signature algorithm on Ether, resulting in a gas consumption value of about 3,400,000. Lastly, we deployed the RCROSS contract specifically designed in this scheme on Ether, which recorded a gas consumption value of roughly 4,700,000. The test data reveal that deploying cross-chain asset transactions requires a considerable amount of smart contract gas. However, when considering identity privacy protection within a single Ether chain, the gas value consumed by the ring signature algorithm is significantly lower than that of deploying cross-chain contracts. Moreover, the gas consumption value of deploying the proposed RCROSS contract remains within an acceptable range when compared to deploying contracts in the relay cross-chain scenario.

5.3.2. RCROSS Contract Function Gas Overhead Comparison

In the testing of the overall gas cost of the scheme, increasing the gas generated by the ring signature algorithm has a significant increase; thus, further analysis is needed with respect to the gas consumption value of the specific algorithm in our proposed scheme. In this section, we tested the main functions used in the RCROSS contract and further analyzed the function with the highest gas consumption value in the RCROSS contract. A comparison of gas consumption values of the function is shown in Figure 4b.

This section measures and compares the gas consumption values of the main functions in the RCROSS contract. From the table above, it can be observed that the gas consumption values of functions related to obtaining transaction information are relatively low, while the gas consumption values of the functions related to transferring cross-chain transactions are relatively high. The gas consumption values of the generation and verification functions of ring signatures are the highest. When testing the gas consumption values of the ring signature algorithm, we tested the generation and replacement signature ringsign() and verified the ring signature verifying() and other functions in the ring signature algorithm, including initialization, key generation, and other algorithms. The gas value consumed during the calculation process cannot be ignored. In summary, the impact of the two core computation and verification ring signature algorithms for identity privacy protection on cross-chain efficiency cannot be ignored. Adding ring signature functionality will have a certain impact on cross-chain efficiency, but, overall, it is within the acceptable range of users.

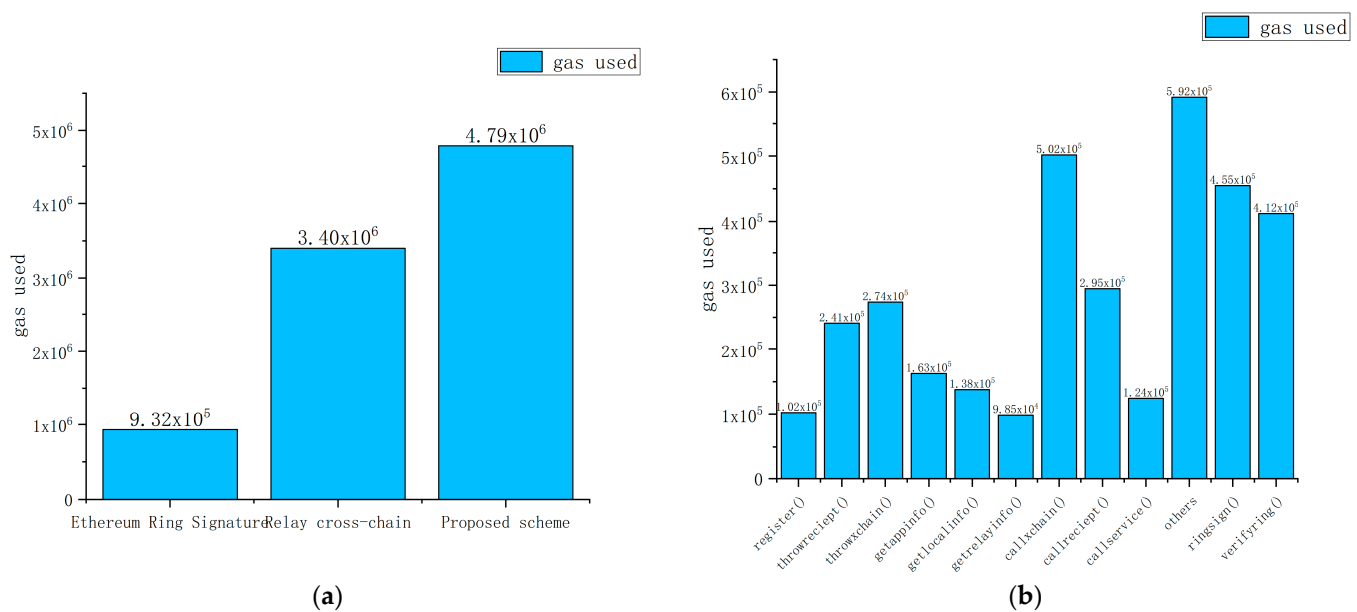


Figure 4. (a) Comparison of Ethereum ring signature, relay cross-chain, and gas consumption of this scheme. (b) In this scheme, the gas consumption values of different functions are compared.

5.3.3. Effect of Increasing the Number of Ring Members on Gas Consumption Values

From the testing of the RCROSS contract function's gas value, we can observe that the gas consumption of functions related to ring signatures in the RCROSS contract is generally high, and the important factor affecting the gas consumption of ring signatures is the number of members in the ring. Therefore, we tested the gas consumption of ring-signature-related functions based on the number of ring members. Figure 5 shows a comparison of the gas consumption of ring signatures.

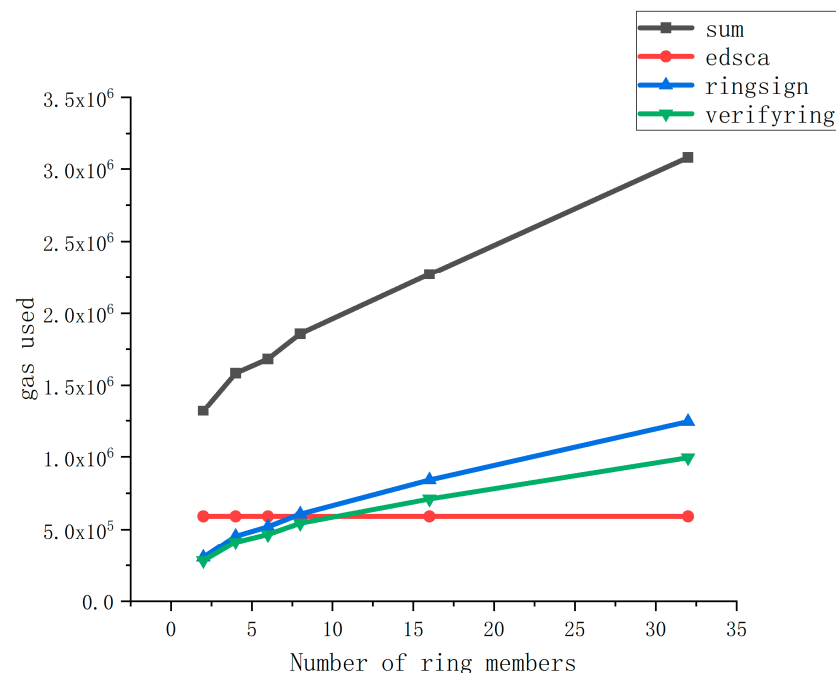


Figure 5. Comparison of ring signature gas consumption values.

We conducted tests to determine the consumed gas when using a ring signature function with varying ring member numbers (specifically, 2, 4, 6, 8, 16, and 32). As the ring

signature algorithm employed in this scheme is based on elliptic curve designs, our test metrics included the gas consumed by the curve, the gas consumed during ring signature generation, and the gas consumed during ring signature verification.

From the chart provided, it is evident that the number of ring members significantly impacts the overall gas consumption. When the number of users falls between 4 and 16, the gas consumed when using the ring signature function remains within an acceptable range, thereby effectively safeguarding user identity privacy. However, it is important to note that users have the freedom to select the number of ring members based on their acceptable gas consumption limits. If users have a greater need for identity privacy, they can appropriately increase the number of ring members.

5.3.4. Transaction Latency Comparison

In this section, we record the transaction latency time of the relay cross-chain scheme and the present scheme that implements identity privacy protection, respectively. The experimental process is to send a simple cross-chain transaction from the source chain to the destination chain. The simple cross-chain transaction sent is to decrease one unit of asset on Ether and increase one unit of asset on Fabric. We record the transaction latency time of the relay cross-chain scheme and the present scheme that implements identity privacy protection, respectively. With respect to transaction latency time, where transaction latency time mainly consists of two metrics, we mainly record the transaction latency required by the relay chain to process a transaction while the transaction is in progress and the transaction latency to process the complete cross-chain transaction, as shown in Figure 6.

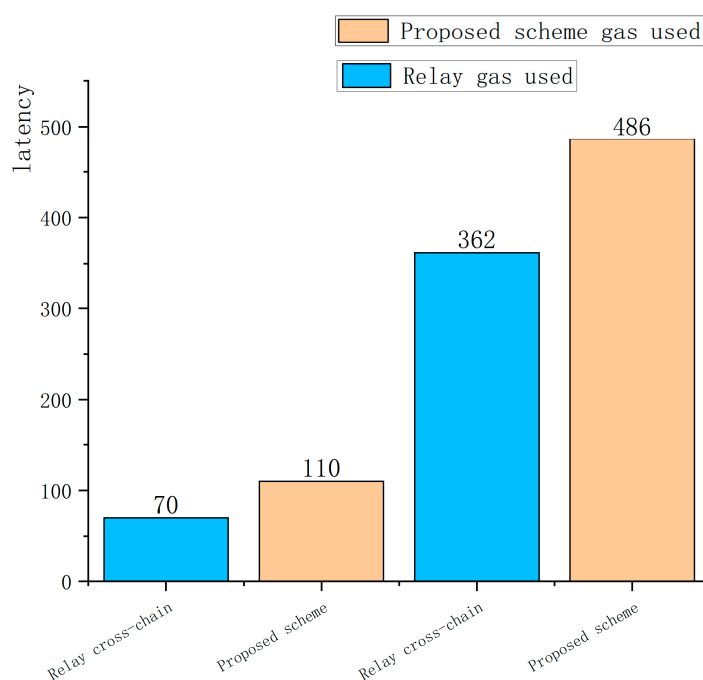


Figure 6. Comparison of latency between relay cross-chain scheme and the proposed scheme.

According to the experimental data, we can see that this scheme has a certain increase in transaction latency compared with the relay cross-chain asset transaction. When initiating a simple transfer transaction from Ether to Fabric, it takes about 70 ms for the relay chain processing system contract, and it takes about 110 ms for the relay chain processing system contract of this scheme with increased identity privacy protection. During transaction execution, the average latency of the relay cross-chain scheme is 362 ms, and the average latency of the present scheme with added identity privacy protection is 486 ms. For individual users, the average transaction latency at this point is acceptable. Therefore,

based on the above record of transaction delay time, we can further conclude that the present scheme has a high degree of practicality for ordinary users with security needs.

The blockchain's impossible triangle theorem makes simultaneously achieving decentralization, security, and scalability difficult. This paper presents a scheme that significantly enhances user identity privacy protection in cross-chain asset transactions, thereby improving security. However, there is a certain decrease in scalability. By conducting a performance evaluation of the scheme, the reduction in transaction performance has been determined to fall within an acceptable range for users. Additionally, the deployment of the RCROSS contract offers the advantage of reusability. This allows for cost reductions by enabling the administrator to set up the contract and deploy it. In the future, users on the application's chain who access the cross-chain network only need to use the functions within the RCROSS contract to facilitate cross-chain transactions.

6. Security Discussions

This scheme mainly achieves identity privacy protection in cross-chain asset-trading scenarios. The ultimate goal of identity privacy protection is to require the nonrelation of the following: the user's identity information; the physical address; the IP address; and public information, such as the user's public key and address on the blockchain. Any unauthorized node cannot obtain any information about the user's identity solely based on the public data on the blockchain, nor can it be monitored through the network. Network technologies, such as traffic analysis, are used to track user transactions and identities. Based on the above design background, we first introduced the characteristics of this scheme for resisting network-layer attacks with respect to other cross-chain schemes and further concluded that this scheme can better resist man-in-the-middle hijacking attacks that application-layer accounts are prone to compared to other schemes.

(1) Network-layer attacks

Reuse attacks: A reuse attack in a blockchain system occurs when a malicious user repeatedly broadcasts a transaction or block that has already been verified in order to deceive other nodes in the network. This attack is often used to compromise identity authentication and steal credentials using network eavesdropping or other methods. The attacker can then resend stolen authentication credentials to the authentication server, thereby stealing identity information. The principle behind a replay attack is to construct an identical data structure in order to obtain the same address, private key, and transaction structure, and then the attack cheats the system. To prevent replay attacks, the scheme proposed in this paper adds a specific, randomly generated number to the requested information and encrypts it. The relay chain then verifies the correctness of the random number, thereby preventing reuse attacks.

(2) Application-layer attacks

Man-in-the-middle hijacking attacks: Man-in-the-middle hijacking attacks often obtain information by eavesdropping on conversations, and then these attacks steal the private account information of legitimate users to impersonate legitimate users and tamper with transactions. Man-in-the-middle hijacking attacks include various methods. In addition to the need for users to improve their security awareness, this scheme achieves maximum resistance to man-in-the-middle attacks. At this point, we assume that the attacker did not obtain a user's personal private key through illegal means and wanted to forge a signature using that user's private key to tamper with the transaction. In the fourth section of this article, it is explained that the ring signature algorithm itself has invisibility, and the probability of attackers forging a legitimate signature after obtaining a single user's private key is very low. This is because in the ring signature algorithm, the verification process of each user's signature in the ring is different, and the signature result is the same. In this case, it greatly increases the complexity of fraud, especially when the user sets the number of ring members to a large number. This can greatly prevent man-in-the-middle attacks.

By analyzing typical network-layer and application-layer attacks, the scheme proposed in this paper exhibits high security in cross-chain asset transaction scenarios, which can ensure the security of accounts holding important transaction information and the network security of transmitting transaction information.

7. Conclusions

As one of the key research directions in the blockchain industry, bridging the underlying architecture gap between different blockchain platforms is a significant challenge. One specific concern when it comes to cross-chain transactions is identity privacy leakage, which has become a pressing issue. To address this issue, this scheme proposes a novel approach by combining the ring signature algorithm with the cross-chain management contract, resulting in the creation of the RCROSS contract. The deployment of the RCROSS contract within the appchain enables the realization of identity privacy protection for cross-chain asset transactions. By leveraging this contract, user identity information is promptly safeguarded, thereby mitigating the risk of any potential identity information leaks. This scheme can be applied not only to cross-chain transactions between homogeneous chains but also to cross-chain transactions between heterogeneous chains without limiting application scenarios. Furthermore, this research conducts performance testing and the security analysis of the proposed scheme.

As researchers continue to improve the ring signature technology, some researchers propose accountable ring signatures [30] and traceable ring signatures [31]. However, considering the limitations of smart contract on-chain computation, we need to balance the security and efficiency of the scheme. In future research, we mainly have two research directions. Firstly, we will improve the ring signature algorithm by using accountable and traceable ring signature algorithms. We will optimize the ring signature algorithm in terms of security and light weight. We will achieve this goal by comparing different ring signature schemes. In addition, we will also attempt to further improve the overall performance of the scheme via a combination of on-chain and off-chain methods. Specifically, we will implement the functions of computing and verifying ring signatures off-chain and integrate them into the underlying architecture of the relay chain to reduce on-chain computation time, lower the difficulty of on-chain computation, improve cross-chain transaction rates, and, ultimately, enhance the scheme's feasibility.

Author Contributions: Conceptualization, S.Z. and R.Z.; methodology, S.Z.; manuscript writing R.Z.; propose research ideas L.W.; validation, S.X. and W.S.; formal analysis, R.Z.; investigation, R.Z.; review and revision S.X.; data collection W.S.; supervision, L.W.; project administration, L.W.; funding acquisition, S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by the Shandong Provincial Natural Science Foundation of China, grant number [ZR2020KF035], the National Natural Science Foundation of China, grant number [62102209], and the Shandong Provincial Key Research and Development Program, grant number [2021CXGC010107].

Data Availability Statement: The datasets used in the current study are available from the corresponding author upon reasonable request.

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

References

1. Guo, Z.; Guo, S.; Zhang, S.; Song, L.; Wang, H. Analysis of cross-chain technology of blockchain. *Chin. J. Internet Things* **2020**, *4*, 35–48.
2. Schulte, S.; Sigwart, M.; Frauenthaler, P.; Borkowski, M. Towards blockchain interoperability. In Proceedings of the 2019 International Conference on Business Process Management, Vienna, Austria, 1–6 September 2019; Springer: Cham, Switzerland, 2019; pp. 3–10.
3. Mendling, J.; Weber, I.; Aalst, W.V.D.; Brocke, J.V.; Cabanillas, C.; Daniel, F.; Debois, S.; Ciccio, C.D.; Dumas, M.; Dustdar, S.; et al. Blockchains for business process management-challenges and opportunities. *ACM Trans. Manag. Inf. Syst. (TMIS)* **2018**, *9*, 4. [[CrossRef](#)]
4. Pan, J.; Huang, D. Blockchain dynamic sharding model based on jump Hash and asynchronous consensus group. *Comput. Sci.* **2020**, *47*, 281–288.

5. Bonneau, J.; Narayanan, A.; Miller, A.; Clark, J.; Kroll, J.A.; Felten, E.W. Mixcoin: Anonymity for bitcoin with accountable mixes. In Proceedings of the Int'l Conference on Financial Cryptography and Data Security, Istanbul, Turkey, 16–17 October 2014; Springer: Berlin, Germany, 2014; pp. 486–504.
6. Chaum, D. Blind signatures for untraceable payments. In Proceedings of the CRYPTO; Springer: Berlin, Germany, 1983; pp. 199–203.
7. Xu, G.; Cao, Y.; Xu, S.; Xiao, K.; Liu, X.; Chen, X.; Dong, M. A Novel Post-Quantum Blind Signature for Log System in Blockchain. *Comput. Syst. Sci. Eng.* **2022**, *41*, 945–958. [\[CrossRef\]](#)
8. Maxwell, G. CoinJoin: Bitcoin Privacy for the Real World. Available online: <https://bitcointalk.org/index.php?topic=279249.0> (accessed on 1 August 2023).
9. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. CoinShuffle: Practical decentralized coin mixing for bitcoin. In Proceedings of the European Symp on Research in Computer Security, Wroclaw, Poland, 7–11 September 2014; Springer: Berlin, Germany, 2014; pp. 345–364.
10. Corrigan-Gibbs, H.; Ford, B. Dissent: Accountable anonymous group messaging. In Proceedings of the ACM Conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; ACM: New York, NY, USA, 2010; pp. 340–350.
11. Ruffing, T.; Moreno-Sanchez, P.; Kate, A. P2P Mixing and unlinkable Bitcoin transactions. In Proceedings of the Network and Distributed System Security Symp. Internet Society, San Diego, CA, USA, 26 February–3 March 2017; pp. 43–58.
12. Ruffing, T.; Moreno-Sanchez, P. ValueShuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin. In *International Conference on Financial Cryptography and Data Security*; Springer: Cham, Switzerland, 2017; pp. 133–154.
13. Ibrahim, M.H. SecureCoin: A Robust Secure and Efficient Protocol for Anonymous Bitcoin Ecosystem. *IJ Netw. Secur.* **2017**, *19*, 295–312.
14. Li, Y.; Yang, G.; Susilo, W.; Yu, Y.; Au, M.H.; Liu, D. Traceable monero: Anonymous cryptocurrency with enhanced accountability. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 679–691. [\[CrossRef\]](#)
15. Saberhagen, N.V. CryptoNote v2.0. Available online: <https://cryptonote.org/whitepaper.pdf> (accessed on 10 August 2023).
16. NIST, FIPS 186-4, Digital Signature Standard. Available online: <https://csrc.nist.gov/publications/detail/fips/186/4/final> (accessed on 10 August 2023).
17. Bernstein, D.J.; Duif, N.; Lange, T.; Schwabe, P.; Yang, B.Y. High-speed high-security signatures. *J. Cryptogr. Eng.* **2012**, *2*, 77–89. [\[CrossRef\]](#)
18. Noether, S.; Mackenzie, A. Ring confidential transactions. *Ledger* **2016**, *1*, 1–18. [\[CrossRef\]](#)
19. Zhang, Z.; Li, W.; Liu, H.; Liu, J. A refined analysis of zcash anonymity. *IEEE Access* **2020**, *8*, 31845–31853. [\[CrossRef\]](#)
20. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous distributed e-cash from bitcoin. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; IEEE: San Francisco, CA, USA, 2014; pp. 397–411.
21. Ben Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from bitcoin. In Proceedings of the IEEE Symposium on Security and Privacy, San Jose, CA, USA, 18–21 May 2014; IEEE: San Francisco, CA, USA, 2014; pp. 459–474.
22. Lin, C.; He, D.; Huang, X.; Khan, M.K.; Choo, K.K.R. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2440–2452. [\[CrossRef\]](#)
23. Cao, L.; Wan, Z. Anonymous scheme for blockchain atomic swap based on zero-knowledge proof. In Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), Dalian, China, 27–29 June 2020; IEEE: San Francisco, CA, USA, 2020; pp. 371–374.
24. Li, Y.; Weng, J.; Li, M.; Wu, W.; Weng, J.; Liu, J.N.; Hu, S. ZeroCross: A sidechain-based privacy-preserving Cross-chain solution for Monero. *J. Parallel Distrib. Comput.* **2022**, *169*, 301–316. [\[CrossRef\]](#)
25. Franklin, M.; Zhang, H. A framework for unique ring signatures. *Cryptol. Eprint Arch.* **2012**, *577*, 1–20.
26. Zamyatin, A.; Harz, D.; Lind, J.; Panayiotou, P.; Gervais, A.; Knottenbelt, W. Xclaim: Trustless, interoperable, cryptocurrency-backed assets. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 20–22 May 2019; pp. 193–210.
27. Borkowski, M.; Sigwart, M.; Frauenthaler, P.; Hukkinen, T.; Schulte, S. DeXTT: Deterministic cross-blockchain token transfers. *IEEE Access* **2019**, *7*, 111030–111042. [\[CrossRef\]](#)
28. Hei, Y.; Li, D.; Zhang, C.; Liu, J.; Liu, Y.; Wu, Q. Practical AgentChain: A compatible cross-chain exchange system. *Future Gener. Comput. Syst.* **2022**, *130*, 207–218. [\[CrossRef\]](#)
29. Pillai, B.; Biswas, K.; Hóu, Z.; Muthukumarasamy, V. Burn-to-claim: An asset transfer protocol for blockchain interoperability. *Comput. Netw.* **2021**, *200*, 108495. [\[CrossRef\]](#)
30. Devidas, S.; Rekha, N.R.; Subba Rao, Y.V. Identity verifiable ring signature scheme for privacy protection in blockchain. *Int. J. Inf. Technol.* **2023**, *15*, 2559–2568. [\[CrossRef\]](#)
31. Perera, M.N.S.; Nakamura, T.; Hashimoto, M.; Yokoyama, H.; Cheng, C.-M.; Sakurai, K. A Survey on Group Signatures and Ring Signatures: Traceability vs. Anonymity. *Cryptography* **2022**, *6*, 3. [\[CrossRef\]](#)

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