PRIVACY-PRESERVING TECHNIQUES FOR SECURE CROSS-CHAIN TRANSACTION

A PROJECT REPORT

Submitted by

RAVI KUMAR B

(2023246037)

A report for the phase-I of the project
submitted to the Faculty of

INFORMATION AND COMMUNICATION ENGINEERING

in partial fulfillment
for the award of the degree
of

MASTER OF TECHNOLOGY

in

INFORMATION TECHNOLOGY

DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING, GUINDY
ANNA UNIVERSITY
CHENNAI 600 025
JANUARY 2025

ANNA UNIVERSITY

CHENNAI - 600 025

BONA FIDE CERTIFICATE

Certified that this project report titled PRIVACY PRESERVING TECHNIQUES FOR SECURE CROSS-CHAIN TRANSACTION is the bona fide work of RAVI KUMAR B who carried out project work under my supervision. Certified further that to the best of my knowledge and belief, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or an award was conferred on an earlier occasion on this or any other candidate.

PLACE:	**DR.J.INDUMATHI**
DATE:	**PROFESSOR**
	PROJECT GUIDE
	DEPARTMENT OF IST, CEG
	ANNA UNIVERSITY
	CHENNAI 600025

COUNTERSIGNED

DR. S. SWAMYNATHAN
HEAD OF THE DEPARTMENT
DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
COLLEGE OF ENGINEERING, GUINDY
ANNA UNIVERSITY
CHENNAI 600025

ABSTRACT

Current cross-chain solutions provide asset transfers between separate blockchains, but they face challenges with privacy breaches and low regulatory compliance. In addition to making regulation and the discovery of illicit activities like money laundering more difficult, privacy-preserving measures frequently increase anonymity. Sensitive information is exposed because to the linkability of transactions across chains, leaving users open to illegal monitoring. Existing methods' practicality is limited by their inability to strike a compromise between privacy and regulation.

The proposed Privacy-Preserving Protocol (PCP) addresses by balancing privacy and traceability for Monero-Bitcoin exchanges. Using cryptographic tools like zero-knowledge proofs and homomorphic commitments, PCP ensures secure, unlinkable transactions while allowing regulators to intervene when necessary. The protocol incorporates selective membership proofs and stealth addresses to enhance privacy without sacrificing accountability, enabling compliance without disrupting legitimate activities. It reduces miners' computational burden and simplifies implementation without relying on trusted hardware.

Experiments show that PCP is efficient, with Monero swaps taking 150 ms, proof generation 40 ms, and verification 24 ms. Tracing takes only 7.12 ms, and the system demonstrates scalability, maintaining performance under varying workloads. These results confirm PCP's cost-effectiveness and practicality in addressing the privacy-regulation trade-off, making it a viable solution for secure and trustworthy blockchain interoperability.

ABSTRACT TAMIL

ACKNOWLEDGEMENT

It is my privilege to express my deepest sense of gratitude and sincere thanks to **Dr. J. INDUMATHI ,** Professor , Department of Information Science and Technology, College of Engineering, Guindy, Anna University, for her constant supervision, encouragement, and support in my project work. I greatly appreciate the constructive advice and motivation that was given to help me advance my project in the right direction.

I am grateful to **Dr. S. SWAMYNATHAN,** Professor and Head, Department of Information Science and Technology, College of Engineering Guindy, Anna University for providing us with the opportunity and necessary resources to do this project.

I would also wish to express my deepest sense of gratitude to the Members of the Project Review Committee: **Dr. S. SRIDHAR,** Professor, **Dr. G. GEETHA,** Associate Professor, **Dr. D. NARASHIMAN,** Teaching Fellow Department of Information Science and Technology,College of Engineering Guindy, Anna University, for their guidance and useful suggestions that were beneficial in helping me improve my project.

I also thank the faculty member and non teaching staff members of the Department of Information Science and Technology, Anna University, Chennai for their valuable support throughout the course of our project work.

RAVI KUMAR B
(2023246037)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

PCP	Privacy-Preserving Protocol
SoK	Signatures Of Knowledge
PoW	Proof of Work
PoS	Proof of Stake
AML	Anti-money laundering
KYC	Know-your-customer
ZKPs	Zero-Knowledge Proofs
IPR	Internet Protocol Routing
IPM	Internet Protocol Masking
RCT	Ring Confidential Transactions
PPBT	Privacy-Preserving Blockchain Transaction

CHAPTER 1

INTRODUCTION

1.1 CROSS-CHAIN TRANSACTIONS AND PRIVACY

Cross-chain transactions enable the transfer of assets and data between different blockchain networks, addressing the isolation of individual blockchains. This capability is crucial as it allows for greater interoperability and utilization of diverse blockchain functionalities. However, cross-chain systems face significant privacy challenges due to the inherent linkability of transactions across different chains. When two blockchains interact, the correlation of their transactions can expose sensitive information, such as the identities of the parties involved and the amounts being transferred, leading to privacy leakage .

Conventional privacy-preserving measures frequently jeopardize regulatory supervision, making it challenging to spot and punish bad actors. Cryptocurrency anonymity can make illicit operations like money laundering and contraband dealing easier. In cross-chain transactions, for example, if one blockchain is compromised, it may have a cascading effect that compromises the privacy of another chain that interacts. This concern emphasizes how important it is to have strong privacy solutions that do not interfere with regulatory compliance.

The goal of recent developments in cryptography is to improve the privacy of cross-chain transactions without compromising legal requirements. The Privacy-Preserving Policy-Enforcement Cross-Chain Protocol (PCP), which combines elements of Bitcoin and Monero, is one such method. To guarantee transaction accuracy and protect user privacy, PCP uses a signature of knowledge (SoK). In addition, it has tools for selective tracing, enabling authorities to remove anonymity when necessary for investigations. Building trust in cross-chain systems and guaranteeing their safe use in a range of applications depend on striking this balance between privacy and regulation.

1.2 DISTRIBUTED STORAGE FOR CROSS-CHAIN TRANSACTIONS

Distributed storage for cross-chain transactions is an innovative approach that enhances the functionality and security of blockchain networks by facilitating seamless communication and asset exchanges between isolated systems. As the blockchain ecosystem continues to expand, the need for interoperability becomes increasingly critical. Distributed storage solutions provide a robust framework for securely storing transaction data across multiple nodes, which not only ensures data integrity but also minimizes the risk of tampering or loss. This decentralized architecture allows for efficient management of transaction volumes, addressing scalability concerns that arise with the growing number of cryptocurrencies and blockchain applications.

Preserving user privacy while guaranteeing regulatory compliance is one of the fundamental obstacles in cross-chain transactions. Transaction details that are shared across blockchains may expose private information about participants and transaction amounts, which is known as privacy leakage. Distributed storage systems can combat this by utilizing sophisticated cryptographic methods like homomorphic encryption and zero-knowledge proofs, which enable transaction verification without revealing particulars. This feature is crucial for safeguarding user identities and stopping criminal actors from using transaction data for illicit purposes like fraud or money laundering.

Additionally, as regulatory scrutiny of cryptocurrencies grows, distributed storage solutions can be developed with compliance capabilities that allow for transaction tracing as needed. Maintaining a secure environment where consumers may transact with confidence across various blockchains requires striking a balance between privacy and regulation. The blockchain ecosystem can meet regulatory requirements, protect user privacy, and increase interoperability by utilizing distributed storage in cross-chain transactions. In the end, this strategy not only improves the performance of DeFi applications but also helps create a blockchain environment that is more reliable and secure.

1.3 BALANCING PRIVACY AND REGULATION IN BLOCKCHAIN

The intricate problem of balancing privacy and regulation in blockchain technology has attracted a lot of interest as the ecosystem grows. The emergence of cross-chain systems, which allow for asset exchange and communication between separate blockchains, has brought attention to the need for practical solutions that preserve user privacy while guaranteeing adherence to legal requirements. Since the correlation of transactions across many blockchains can reveal private information about participants, such as their identities and transaction amounts, privacy leakage is still a serious risk. Conventional privacy-preserving measures can unintentionally jeopardize regulatory supervision, making it more challenging to spot and punish bad actors involved in illicit activities like fraud or money laundering. This makes the need for novel protocols that protect privacy without compromising the ability to enforce laws urgent.

The Privacy-Preserving Policy-Enforcement Cross-Chain Protocol (PCP), which was developed in response to recent developments, attempts to successfully address these issues. PCP combines elements of more open systems like Bitcoin with privacy-focused cryptocurrencies like Monero. PCP enables users to validate transactions without disclosing their identities or transaction data by utilizing cryptographic techniques like stealth addresses and signatures of knowledge (SoK). The protocol's methods for selective tracing are crucial because they allow regulatory bodies to remove anonymity when needed for investigations. This two-pronged strategy guarantees that consumers have some privacy while maintaining a channel for responsibility in the event of wrongdoing.

In cross-chain transactions, the use of PCP shows a promising balance between privacy and regulation. The protocol functions effectively, according to experimental data, with little delay in transaction processing and proof verification. In addition to increasing user trust, PCP creates a more secure environment for cross-chain transactions by resolving privacy concerns and regulatory constraints. Such creative solutions will be essential to creating a sustainable ecosystem that protects user privacy and complies with relevant legal frameworks as blockchain technology develops further. This will ultimately help blockchain applications become more widely accepted and integrated across a range of industries.

1.4 BLOCKCHAIN

The blockchain technologies most relevant to the discussion of balancing privacy and regulation in cross-chain transactions are Monero and Bitcoin. Monero is a decentralized cryptocurrency that prioritizes user privacy through advanced cryptographic techniques, including ring signatures, stealth addresses, and range proofs. These features make it extremely difficult to trace transactions, thereby protecting the identities of senders and receivers as well as the amounts involved. This high level of anonymity, while beneficial for user privacy, poses challenges for regulatory compliance, particularly in preventing illegal activities such as money laundering and fraud. The integration of Monero in cross-chain systems allows for the implementation of privacy-preserving protocols that can still accommodate regulatory oversight when necessary.

In contrast, Bitcoin is a well-known cryptocurrency transaction framework that is frequently used in cross-chain protocols because of its strong security features and well-established infrastructure. When it comes to striking a balance between privacy and regulation, Bitcoin's open ledger makes it simpler to track transactions, which is crucial for regulatory compliance. These two blockchains can cooperate, as demonstrated by the proposed Privacy-Preserving Policy-Enforcement Cross-Chain Protocol (PCP). Under typical conditions, PCP preserves user anonymity while enabling selective transaction tracing by utilizing both Bitcoin's regulatory powers and Monero's privacy features. A more secure and reliable blockchain environment will eventually be fostered by this collaboration between Monero and Bitcoin, which shows a promising way to strike a balance between user privacy and the required regulatory monitoring in cross-chain transactions.

1.4.1 Structure of Blockchain

- Blocks: Each block contains a list of transactions, a timestamp, and a cryptographic hash of the previous block. This hash links the blocks together, ensuring that any alteration of a block would invalidate all subsequent blocks, thus maintaining the integrity of the data.

- Nodes: The blockchain operates on a network of nodes, which are computers that maintain a copy of the entire blockchain. Nodes validate transactions and blocks through consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), ensuring that only legitimate transactions are added to the blockchain.

- Consensus Mechanisms: These are protocols used by nodes to agree on the validity of transactions. They prevent double-spending and ensure that all copies of the blockchain remain synchronized across the network. Different blockchains may employ different consensus algorithms depending on their design goals and security needs.

- Smart Contracts: In addition to simple transactions, many blockchains support smart contracts—self-executing contracts with the terms directly written into code. These contracts automatically enforce and execute agreements when predefined conditions are met, enabling complex interactions between users without intermediaries.
- Cryptography: Blockchain security relies heavily on cryptographic techniques to secure data and control access. Public and private keys are used to facilitate secure transactions between parties while maintaining anonymity.

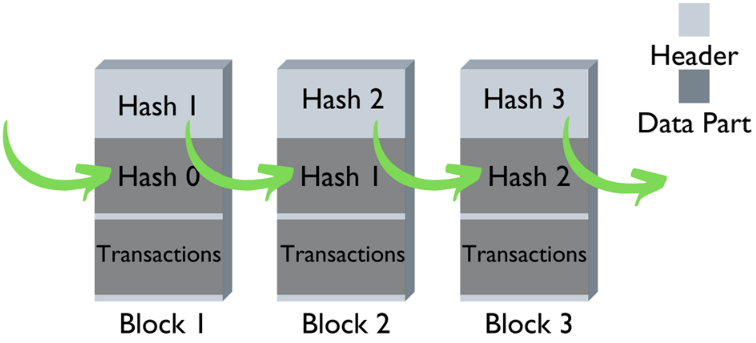


Figure 1.1: Structure of Blockchain

1.4.2 Consensus mechanism

Consensus mechanisms are fundamental components of blockchain technology, ensuring that all participants in a decentralized network agree on the validity of transactions and the state of the blockchain. They are essential for maintaining the integrity and security of the blockchain while preventing issues such as double-spending. Different consensus mechanisms have been developed, each with its unique approach to achieving agreement among nodes, and they can generally be categorized into two main types: Proof of Work (PoW) and Proof of Stake (PoS).

- Proof of Work (PoW) is the consensus mechanism originally introduced by Bitcoin. In PoW, miners compete to solve complex mathematical problems, and the first one to find a solution gets to add a new block to the blockchain and is rewarded with cryptocurrency. This process requires significant computational power and energy consumption, which raises concerns about environmental sustainability. However, PoW has proven effective in securing networks against attacks, as altering any part of the blockchain would require an enormous amount of computational resources to re-mine all subsequent blocks.
- Proof of Stake (PoS) offers a more energy-efficient alternative by allowing validators to create new blocks based on the number of coins they hold and are willing to ”stake” as collateral. This mechanism reduces the need for extensive computational work, making it less resource-intensive than PoW. Validators are chosen to create new blocks and verify transactions based on their stake in the network, incentivizing them to act honestly since they have something to lose. PoS has gained popularity in newer blockchain projects due to its scalability and lower energy consumption.

1.4.3 Cryptographic Techniques

Cryptographic techniques are foundational to ensuring security, privacy, and integrity in blockchain systems, particularly in the context of cross-chain transactions. These techniques enable users to conduct transactions without revealing sensitive information while maintaining the ability to verify the legitimacy of those transactions. Key cryptographic methods employed in blockchain include ring signatures, stealth addresses, range proofs, commitment schemes, and signatures of knowledge (SoK).

- Ring signatures: allow a group of signers to sign a message on behalf of the group without revealing which member signed it. This technique is integral to privacy-focused cryptocurrencies like Monero, as it obscures the identity of the transaction sender while still providing proof that the transaction is valid.
- Stealth addresses: further enhance privacy by generating unique one-time addresses for each transaction, ensuring that only the intended recipient can access the funds.
- Range proofs: allow a sender to prove that a transaction amount is within a specified range without disclosing the exact amount, thereby preventing potential exploitation of transaction data.
- Signature of knowledge (SoK): enables a user to demonstrate possession of specific information (such as a private key) without disclosing that information itself. This technique supports privacy while allowing verification of transaction correctness.

1.5 NEED FOR PRIVACY PRESERVING PROTOCOL

The need for privacy-preserving protocols in blockchain systems has become increasingly critical as the use of cryptocurrencies expands and cross-chain transactions gain traction. As isolated blockchains begin to communicate and exchange assets, the potential for privacy leakage rises significantly. Cross-chain systems, particularly those utilizing sidechains, often expose transaction details such as the identities of parties involved and the amounts being transferred. This linkability can lead to severe privacy violations, where malicious actors could exploit this information for illegal activities, including identity theft and financial fraud. Traditional privacy-preserving techniques, while effective in securing individual transactions, often fall short in addressing the regulatory requirements necessary for monitoring and controlling illicit activities within these networks.

In order to overcome these obstacles, a strong privacy-preserving policy-enforcement protocol (PCP) is necessary. PCP seeks to strike a compromise between user privacy requirements and regulatory control requirements. PCP enables users to validate transactions without disclosing private information by utilizing sophisticated cryptographic techniques like signatures of knowledge (SoK). This approach guarantees that users can keep their privacy intact during cross-chain transactions, but that a system for accountability and tracing is still in place in case it becomes necessary. Building confidence between users and regulators is made possible by this dual approach, which offers a framework in which privacy does not imply a lack of monitoring.

Moreover, implementing a privacy-preserving protocol like PCP can significantly enhance the overall security and functionality of cross-chain systems. By incorporating features that allow for selective tracing of transactions, PCP enables regulatory authorities to intervene only when necessary, thus preserving user anonymity under normal circumstances. This balance is vital for encouraging wider adoption of blockchain technology across various sectors while ensuring compliance with legal standards. Ultimately, as blockchain continues to evolve, the integration of privacy-preserving protocols will be fundamental in creating a secure, efficient, and trustworthy environment for cross-chain transactions.

1.6 ORGANIZATIONOFTHEREPORT

This report is organized into 6 chapters, describing each part of the project with detailed illustrations and system design diagrams.

CHAPTER 2: Literature Review reviews existing research, studies, and relevant literature related.
CHAPTER 3: System Design describes the design of the project. It explains the architecture, components, algorithms, and any other technical details.
CHAPTER 4: Implementation provides details about how the project was implemented. It discusses the tools, technologies, programming languages, and frameworks used.
CHAPTER 5: Results and Analysis presents the results of the project. It analyzes the outcomes, compares them with expectations, and discusses any challenges faced during implementation.
CHAPTER 6: Conclusions and Future Work summarizes the findings and draws conclusions. It discusses the significance of the work and its implications.

CHAPTER 2

LITERATURE SURVEY

2.1 OVERVIEW

This chapter reviews existing work in the domains of privacy-preserving cross-chain transactions, cryptographic tools for secure exchanges, blockchain interoperability, and regulatory mechanisms for cryptocurrency systems. The survey focuses on sidechain-based solutions for cross-chain interactions, advanced cryptographic techniques like Signatures of Knowledge (SoK) and homomorphic commitments, privacy-preserving mechanisms to ensure unlinkability, and frameworks enabling selective anonymity revocation for regulatory compliance. Additionally, it explores the implementation of efficient proof generation and verification methods for scalable blockchain systems. Include the limitations of the existing work and briefly explain how your idea is advantageous over the existing ones in this chapter.

2.2 INTERCHAIN EXCHANGE AND CONFIDENTIALITY

Cross-chain transactions enable seamless asset transfers and data sharing between isolated blockchain networks, addressing interoperability challenges inherent in traditional blockchain systems. However, these transactions introduce significant privacy concerns. The public and transparent nature of blockchain networks means that cross-chain interactions can reveal sensitive information, such as user identities and transaction details, which can be exploited by malicious actors for identity theft, fraud, or other cybercrimes.

Privacy preservation is, therefore, a critical consideration in the design of cross-chain systems [1][2].

To address these challenges, advanced cryptographic techniques have been integrated into cross-chain protocols. Zero-Knowledge Proofs (ZKPs), such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) and zk-STARKs, have emerged as key solutions. ZKPs allow users to prove the validity of a transaction without disclosing any details about it, thereby maintaining confidentiality. These techniques have been widely adopted in privacy-focused blockchains like Zcash and are increasingly being used in cross-chain protocols to ensure secure and private interactions between networks [3][4]. Additionally, ring signatures, as implemented in Monero, obscure the identity of the transaction sender by blending their transaction with others in a group. This ensures that the source of a transaction cannot be easily traced, providing anonymity while preserving transaction integrity[5].

Despite these advancements, achieving a balance between privacy and regulatory compliance remains a challenge. Techniques such as regulatory trapdoors, which allow authorities to selectively access transactional details under predefined legal conditions, have been proposed to address this issue. These mechanisms ensure that privacy-preserving cross-chain systems remain compliant with anti-money laundering (AML) and know-your-customer (KYC) regulations, providing a secure yet accountable environment for users [6]. As research and development in this field continue, the integration of scalable cryptographic solutions is expected to enhance the usability and security of cross-chain systems, solidifying their role in the broader blockchain ecosystem[7].

2.3 ANONYMITY-ENSURING TECHNIQUES FOR BLOCKCHAIN TRANSACTIONS

Privacy-preserving protocols for blockchain transactions are critical for enhancing user anonymity, securing sensitive data, and ensuring compliance with regulatory standards. These protocols employ advanced cryptographic methods to conceal transaction details while enabling seamless and verifiable exchanges. Techniques like zero-knowledge proofs (ZKPs) allow users to validate transactions without revealing private information, exemplified by zk-SNARKs, widely used in privacy-focused cryptocurrencies such as Zcash[2][4][4]. Homomorphic encryption enables operations on encrypted data, ensuring privacy even during computational processes. Stealth addresses, a prominent feature in protocols like HE-DKSAP, ensure one-time, unlinkable addresses for each transaction, thereby mitigating risks of identity exposure. Differential privacy, which introduces statistical noise to transactional data, allows for aggregate analysis without compromising individual privacy[8].

Furthermore, mechanisms such as cryptographic accumulators and privacy-preserving data aggregation systems facilitate secure data exchange and verification while preserving confidentiality. Selective traceability features, like trapdoor mechanisms, empower authorized entities to revoke anonymity when necessary, striking a balance between privacy and accountability. Collectively, these privacy-preserving protocols are transforming blockchain ecosystems, making them more secure and user-friendly while addressing critical privacy concerns[3].

2.4 CONFIDENTIAL TRANSACTION PROTOCOLS FOR CROSS-CHAIN

To address privacy challenges, advanced cryptographic techniques have been integrated into cross-chain systems, enabling secure transactions without compromising user confidentiality. Bulletproofs, for example, provide compact zero-knowledge proofs that verify transaction validity without revealing sensitive information [2]. These proofs reduce the computational and storage overhead associated with traditional zero-knowledge systems, making them ideal for cross-chain applications . zk-SNARKs, another powerful cryptographic tool, have been employed in protocols like Zendoo to allow decentralized verification of cross-chain transactions while ensuring the privacy of user data [4][3].

Additionally, privacy-focused systems like ZeroCross target specific vulnerabilities in Monero-based cross-chain solutions by employing accumulators to obfuscate transaction details[8]. Accumulators allow users to prove membership in a set without revealing the specific element, ensuring anonymity during cross-chain exchanges. These mechanisms not only enhance privacy but also address scalability concerns by optimizing computational efficiency. However, implementing these solutions requires careful consideration of trade-offs between security, efficiency, and usability[3].

2.5 FRAMEWORKS FOR BLOCKCHAIN

Blockchain integration frameworks in existing systems aim to enhance functionality, transparency, and efficiency across various industries. One proposed solution aligns blockchain systems with organizational objectives, ensuring seamless integration and optimal performance. Another approach incorporates blockchain-based applications as modular extensions within existing infrastructures, leveraging the decentralized nature of blockchain to improve data management and distribute business logic effectively, as demonstrated in practical case studies. In the supply chain domain, specific frameworks focus on increasing transparency and efficiency, enabling enhanced traceability and accountability[9].

Additionally, platforms like Hyperledger Fabric offer permissioned blockchain infrastructures with modular architectures that allow for configurable consensus and membership services, making them adaptable to diverse organizational needs. These frameworks highlight the potential of blockchain to transform existing systems by promoting trust, improving data integrity, and streamlining operations[10].

2.6 FRAMEWORKS FOR CROSS-CHAIN

Cross-sidechain systems are essential for achieving interoperability and seamless communication between independent blockchain networks. These frameworks enable the transfer of assets, data, and smart contract interactions across sidechains, which operate as auxiliary chains connected to a main blockchain. A robust cross-sidechain framework must address challenges such as ensuring transaction atomicity, maintaining data integrity, and preserving user privacy while optimizing scalability and performance [1][2].

Several approaches to cross-sidechain frameworks have been proposed, leveraging innovative technologies and protocols. One notable example is the use of pegged sidechains, where assets are transferred between chains using a two-way peg mechanism. This approach locks assets on the main chain while releasing equivalent assets on the sidechain, ensuring secure and verifiable asset migration. The Bitcoin sidechain framework, known as Rootstock (RSK), exemplifies this concept, allowing smart contract functionality to be integrated with the Bitcoin network [11].

Another significant development is the adoption of relay-based frameworks, where a relay node monitors events on one blockchain and triggers corresponding actions on another. Polkadot's relay chain is a prominent example, providing a shared security model for interconnected parachains while enabling cross-chain communication. Similarly, Cosmos utilizes the Inter-Blockchain Communication (IBC) protocol, facilitating secure data exchange between heterogeneous blockchains while maintaining scalability and flexibility [12].

Despite these advancements, achieving full interoperability and standardization across diverse blockchain ecosystems remains a challenge. Ongoing research focuses on developing universal standards and APIs for cross-sidechain communication, alongside addressing issues like high computational costs and network latency. As these frameworks evolve, they are expected to play a pivotal role in fostering a more interconnected and scalable blockchain ecosystem[13].

2.7 RESEARCH GAPS IDENTIFIED

The literature review comprehensively explores the transformative potential of cross-chain systems in addressing blockchain interoperability challenges. These systems enable seamless asset transfers, data sharing, and smart contract execution across isolated blockchain networks, fostering a more interconnected ecosystem. Privacy preservation is a central focus, with advanced cryptographic techniques such as Zero-Knowledge Proofs (ZKPs), stealth addresses, and ring signatures ensuring transaction confidentiality while maintaining system integrity. However, balancing privacy with regulatory compliance remains a critical challenge, as frameworks must prevent misuse of anonymity for illegal activities while adhering to anti-money laundering (AML) and know-your-customer (KYC) regulations.

Scalability and interoperability are also key areas of research. Techniques like sharding, Layer 2 solutions, and hybrid consensus mechanisms address the limitations of traditional blockchains, allowing cross-chain systems to process large transaction volumes efficiently. Frameworks such as Polkadot's relay chain and Cosmos' Inter-Blockchain Communication (IBC) protocol exemplify innovative approaches to secure and flexible cross-chain communication. These systems integrate cryptographic tools, such as accumulators and regulatory trapdoors, to ensure efficient, secure, and privacy-preserving interactions between heterogeneous blockchains.

Despite significant progress, challenges such as computational overheads, network latency, and the lack of universal standards persist. Future research focuses on enhancing the scalability, interoperability, and usability of cross-chain systems through advanced technologies like post-quantum cryptography, adaptive privacy mechanisms, and AI-driven analytics. As these frameworks continue to evolve, they hold the potential to redefine blockchain ecosystems, enabling secure, scalable, and user-centric solutions across industries ranging from finance to healthcare and supply chain management.

2.8 PROBLEM STATEMENT

The increasing adoption of blockchain technologies and cryptocurrencies, cross-chain systems have become essential for enabling interactions and asset exchanges between isolated blockchains. However, these systems face significant challenges in preserving user privacy while allowing for effective regulation. Current solutions often compromise one for the other, leading to vulnerabilities such as privacy leaks or insufficient mechanisms to trace malicious activities. The problem lies in achieving a balance between ensuring transaction anonymity and providing traceability for regulatory compliance, particularly in cross-chain exchanges between privacy-focused cryptocurrencies like Monero and public ones like Bitcoin.

2.9 OBJECTIVES OF PROPOSED SYSTEM

- To enable seamless and privacy-preserving cross-chain transactions between blockchains like Monero and Bitcoin using a secure protocol.
- To mitigate privacy leakage in cross-chain systems by implementing unlinkability mechanisms that protect user identities and transaction details.
- To balance user privacy and regulatory requirements by incorporating a selective traceability feature for authorized investigations.
- To leverage cryptographic techniques such as the signature of knowledge (SoK) and accumulators to ensure the correctness of transactions without revealing sensitive details.
- To ensure the anonymity of payers while preventing malicious activities through a passive and optimistic tracing authority.
- To develop an efficient and cost-reasonable cross-chain transaction protocol with formal security proofs for anonymity, traceability, and unlinkability.
- To provide a secure mechanism for addressing the risks of linkability and remote side-channel attacks in cross-chain exchanges.

- To conduct experiments to validate the performance and cost-effectiveness of the proposed protocol under practical conditions.

CHAPTER 3

SYSTEM DESIGN

3.1 ARCHITECTURE OF PPBT SYSTEM

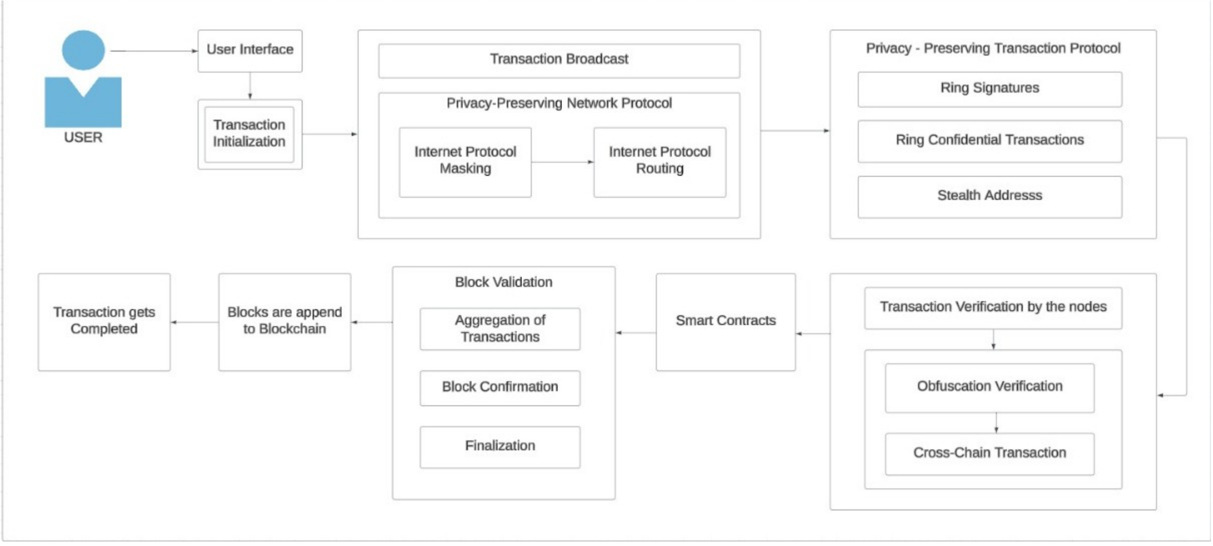

USER
User Interface
Transaction Initialization
Transaction Broadcast
Privacy-Preserving Network Protocol
Internet Protocol Masking
Internet Protocol Routing
Privacy - Preserving Transaction Protocol
Ring Signatures
Ring Confidential Transactions
Stealth Addresss
Transaction Verification by the nodes
Obfuscation Verification
Cross-Chain Transaction
Smart Contracts
Block Validation
Aggregation of Transactions
Block Confirmation
Finalization
Blocks are append to Blockchain
Transaction gets Completed

Figure 3.1: Architectural of PPBT System

3.2 USER INTERFACE MODULE

The User Interface serves as the primary point of interaction for users to initialize and manage blockchain transactions. It is designed to provide a secure and intuitive platform, enabling users to input transaction details with ease while ensuring their privacy is maintained. By integrating seamlessly with underlying privacy-preserving protocols, the interface offers a user-friendly experience, allowing users to perform transactions confidently and efficiently.

3.2.1 Transaction Initialization

The Transaction Initialization Function is responsible for collecting user inputs, such as transaction details (amount, recipient, and other metadata), through the user interface. It generates a unique transaction ID and ensures the data is securely encrypted to maintain user privacy

3.2.2 Transaction Broadcast

Transaction Broadcast process is a critical step in the blockchain workflow, responsible for securely transmitting transaction data across the network. It leverages a Privacy-Preserving Network Protocol, which incorporates Internet Protocol (IP) Masking and IP Routing to ensure anonymity and prevent traceability of transaction origins. This layer of privacy safeguards user identities and protects sensitive data from potential breaches. By disseminating transactions efficiently and securely, the broadcast process ensures that all network nodes receive the necessary information while upholding high standards of confidentiality and decentralization.

3.3 PRIVACY PRESERVING NETWORK PROTOCOL MODULE

The Privacy-Preserving Network Protocol is a foundational component designed to ensure secure and anonymous communication within the blockchain ecosystem. It employs Internet Protocol (IP) Masking, which conceals the user’s actual IP address, preventing tracking or identification of transaction origins. Additionally, IP Routing adds another layer of privacy by relaying transactions through multiple network nodes, making it nearly impossible to trace their path. Together, these mechanisms protect user identities and transaction data from surveillance or malicious actors. This protocol ensures that privacy remains intact without compromising the efficiency or reliability of the network.

3.3.1 Internet Protocol Masking

Internet Protocol (IP) Masking ensures user privacy by concealing their actual IP address during transaction processes. This is achieved by routing the user's data through intermediary nodes, making it challenging to trace the origin of the transaction. It serves as a critical layer in maintaining anonymity within privacy-preserving networks.

3.3.2 Internet Protocol Routing

Internet Protocol (IP) Routing ensures efficient and secure transmission of transaction data across the network. It directs data packets through optimized pathways while maintaining privacy by avoiding exposure of the user's original location. This process works alongside IP Masking to enhance anonymity and safeguard sensitive information.

3.4 PRIVACY PRESERVING TRANSACTION PROTOCOL MODULE

The Privacy-Preserving Transaction Protocol secures user anonymity and transaction confidentiality through advanced cryptographic techniques. It employs methods such as Ring Signatures, Ring Confidential Transactions, and Stealth Addresses to obscure transaction details, including sender, receiver, and amounts, ensuring complete privacy while maintaining blockchain integrity.

3.4.1 Ring Signatures

Ring Signatures are cryptographic tools used in privacy-preserving protocols to conceal the identity of the sender in a transaction. They allow a signer to be part of a group (or ring) of potential signers, making it computationally infeasible to determine which member signed the transaction. This ensures anonymity while maintaining transaction authenticity.

3.4.2 Ring Confidential Transaction

Ring Confidential Transactions (RingCT) enhance privacy by concealing the amount transferred in a transaction. They combine ring signatures with cryptographic techniques to ensure that transaction amounts are hidden while still being verifiable by the network. This ensures both confidentiality and trust in the transaction process.

3.4.3 Stealth Addresses

Stealth Addresses enhance transaction privacy by generating unique, one-time addresses for each transaction. This prevents linking multiple transactions to a single user, safeguarding their identity and financial activities. Only the recipient can recognize and access the funds associated with the stealth address.

3.5 TRANSACTION VERIFICATION BY THE NODES

Transaction Verification by the nodes ensures the legitimacy and accuracy of transactions within the network. Nodes validate transactions through processes like obfuscation verification and cross-chain transaction checks. This decentralized verification mechanism enhances security, maintains trust, and prevents fraudulent activities.

3.5.1 Obfuscation Verification

Obfuscation Verification ensures the privacy of transactions by validating the use of cryptographic methods that conceal sensitive details like sender, receiver, and transaction amount. It confirms that the obfuscation techniques, such as encryption and masking, are correctly applied without compromising data integrity or network security.

3.5.2 Cross-Chain Transactions

Cross-Chain Transactions enable the transfer of assets or data between different blockchain networks. They ensure interoperability by verifying and securely executing transactions across chains without compromising privacy. This allows seamless interaction between diverse blockchain ecosystems.

3.6 SMART CONTRACT

Smart Contracts are self-executing programs that automatically enforce and execute predefined conditions within a transaction. They operate on the blockchain, ensuring transparency, efficiency, and trust without the need for intermediaries. These contracts play a vital role in automating processes while maintaining security and accuracy.

3.7 BLOCK VALIDATION

The Block Validation process ensures the integrity and legitimacy of data before it is permanently recorded on the blockchain. It begins with the aggregation of transactions, where pending transactions are collected and organized into a block structure. Next, the block undergoes confirmation to ensure it complies with the consensus rules and is deemed valid. Finally, the process concludes with finalization, marking the block as complete and immutable, preparing it for inclusion in the blockchain. This sequence is crucial for maintaining the reliability and trustworthiness of the blockchain network.

3.7.1 Aggregation of Transactions

The Aggregation of Transactions step involves collecting and organizing pending transactions into a structured format suitable for inclusion in a block. This process ensures that all valid transactions are efficiently grouped, prioritized, and prepared for further validation. It is a critical step in optimizing the block creation process and maintaining the smooth operation of the blockchain network.

3.7.2 Block Confirmation

The Block Confirmation process involves verifying that the newly created block adheres to the blockchain's consensus rules and protocols. This includes checking the validity of transactions, ensuring there are no double-spends, and confirming that the block's cryptographic hash meets the required difficulty level. Once verified, the block is approved for finalization.

3.7.3 Blocks are append to Blockchain

The Blocks are appended to Blockchain step involves adding the validated and finalized block to the existing blockchain. This process ensures the block becomes a permanent, immutable part of the distributed ledger. Once appended, the block's data is securely linked to the previous blocks, maintaining the integrity and continuity of the blockchain.

3.8 TRANSACTION COMPLETION

The Transaction Completion step marks the finalization of a transaction after its inclusion in a validated and appended block on the blockchain. At this stage, the transaction is considered confirmed and immutable, ensuring its details are securely recorded. This completion provides assurance to all parties involved that the transaction is successfully processed.

3.9 HARDWARE REQUIREMENTS

- **Processor:** Intel i5 or above.
- **RAM:** 8GB(minimum)
- **Storage:** SSD with at least 10 GB of free space

3.10 SOFTWARE REQUIREMENTS

- **Blockchain Platform:** A blockchain framework such as Monero for implementing privacy-preserving transactions.

- **Monero Testnet Tools:** For creating and managing testnet accounts and dummy transactions.
- **CryptoNote:** Protocol for enabling privacy features like ring signatures and stealth addresses.
- **Tor:** For implementing Internet Protocol Masking to ensure privacy in transaction routing.
- **Python/JavaScript SDKs:** Libraries for integrating Monero or other blockchain features into the application.
- **React:** For building the user interface to initialize and track transactions.
- **Node.js:** For backend services, API development, and interacting with blockchain nodes.
- **Monero Daemon:** For running a local Monero node for transaction validation and network interactions.
- **OpenSSL or Libsodium:** Cryptographic libraries for secure data processing and signing transactions.
- **Docker:** For containerizing the application and managing test environments.
- **Testing Frameworks:** Tools like Mocha, Jest, or similar for validating smart contract functionality and privacy protocols.

CHAPTER 4

IMPLEMENTATION

4.1 DATA FLOW DIAGRAM

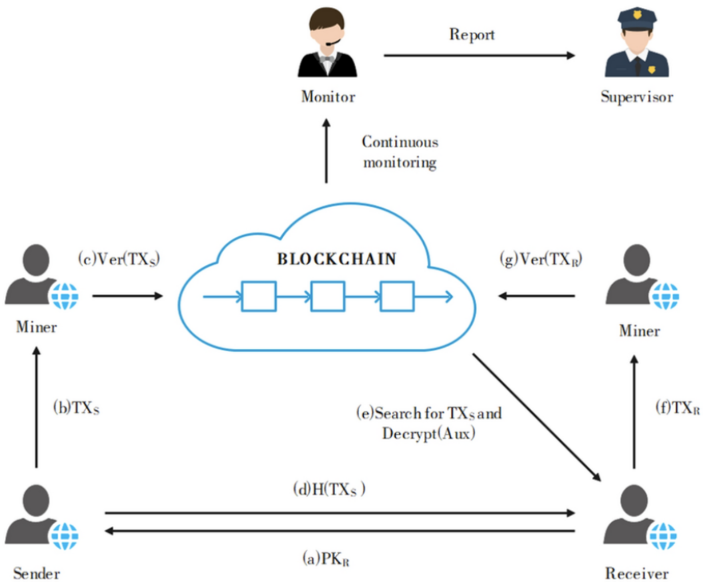


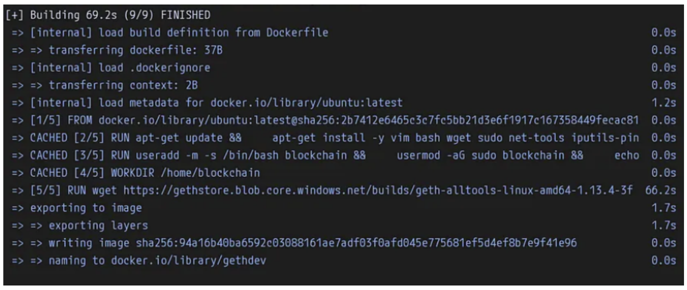
Figure 4.1: Data flow diagram of Privacy Transactions

In Figure.4.1 the Data flow Diagram illustrates a secure transaction workflow using a blockchain network. The process starts with the sender creating and encrypting a transaction, which is then transmitted to the network. Miners validate the transaction and store it on the blockchain. A monitoring system continuously oversees the network, ensuring proper functioning and generating reports for oversight authorities. The recipient retrieves the encrypted transaction from the network, decrypts it, and verifies its authenticity. Miners confirm the transaction's integrity before the recipient completes the process. This workflow ensures secure communication, data integrity, and oversight throughout the transaction lifecycle.

4.2 CROSS-CHAIN DEVELOPMENT AND DEPLOYMENT

4.2.1 Starting up the Docker Container

In figure.4.2 starting up a Docker container involves using the **docker run** command to launch a container based on a predefined image. This command initializes the container with all the necessary configurations, dependencies, and blockchain components specified in the Dockerfile. Once started, the container operates in an isolated environment, enabling seamless interaction with the blockchain network.

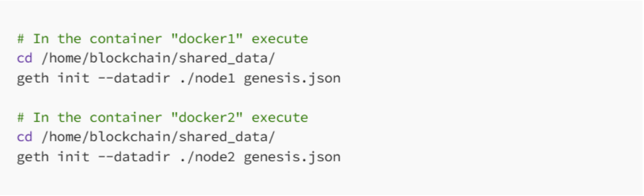


```
[+] Building 69.2s (9/9) FINISHED
 => [internal] load build definition from Dockerfile                                          0.0s
 => => transferring dockerfile: 37B                                                           0.0s
 => [internal] load .dockerignore                                                             0.0s
 => => transferring context: 2B                                                               0.0s
 => [internal] load metadata for docker.io/library/ubuntu:latest                              1.2s
 => [1/5] FROM docker.io/library/ubuntu:latest@sha256:2b7412e6465c3c7fc5bb21d3e6f1917c167358449fecac81  0.0s
 => CACHED [2/5] RUN apt-get update &&     apt-get install -y vim bash wget sudo net-tools iputils-pin  0.0s
 => CACHED [3/5] RUN useradd -m -s /bin/bash blockchain &&     usermod -aG sudo blockchain &&     echo  0.0s
 => CACHED [4/5] WORKDIR /home/blockchain                                                     0.0s
 => [5/5] RUN wget https://gethstore.blob.core.windows.net/builds/geth-alltools-linux-amd64-1.13.4-3f  66.2s
 => exporting to image                                                                        1.7s
 => => exporting layers                                                                       1.7s
 => => writing image sha256:94a16b40ba6592c03088161ae7adf03f0afd045e775681ef5d4ef8b7e9f41e96   0.0s
 => => naming to docker.io/library/gethdev                                                    0.0s
```

Figure 4.2: Starting up the Docker Container

4.2.2 Initializing the nodes

In figure4.3 docker initialization in blockchain transactions involves setting up a containerized environment to streamline the development, deployment, and management of blockchain networks. Docker allows developers to package the blockchain application, including all dependencies such as privacy protocols, smart contracts, and node configurations, into lightweight containers. This ensures consistency across different environments, from development to production.



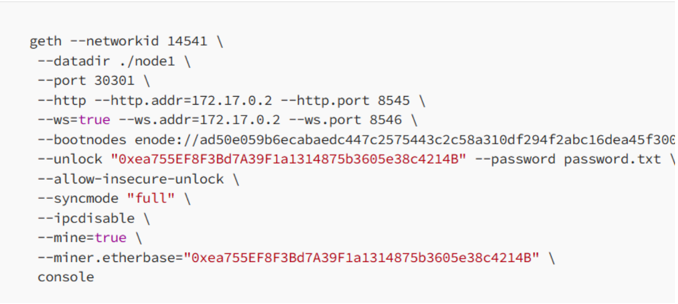
```
# In the container "docker1" execute
cd /home/blockchain/shared_data/
geth init --datadir ./node1 genesis.json

# In the container "docker2" execute
cd /home/blockchain/shared_data/
geth init --datadir ./node2 genesis.json
```

Figure 4.3: Initializing the nodes

4.2.3 Starting the nodes

In figure4.4 starting the nodes involves specifying several parameters to the geth command. Below is the command you can execute to fire up node1 in the container docker1. Chang to the folder /home/blockchain/shared data before executing this.

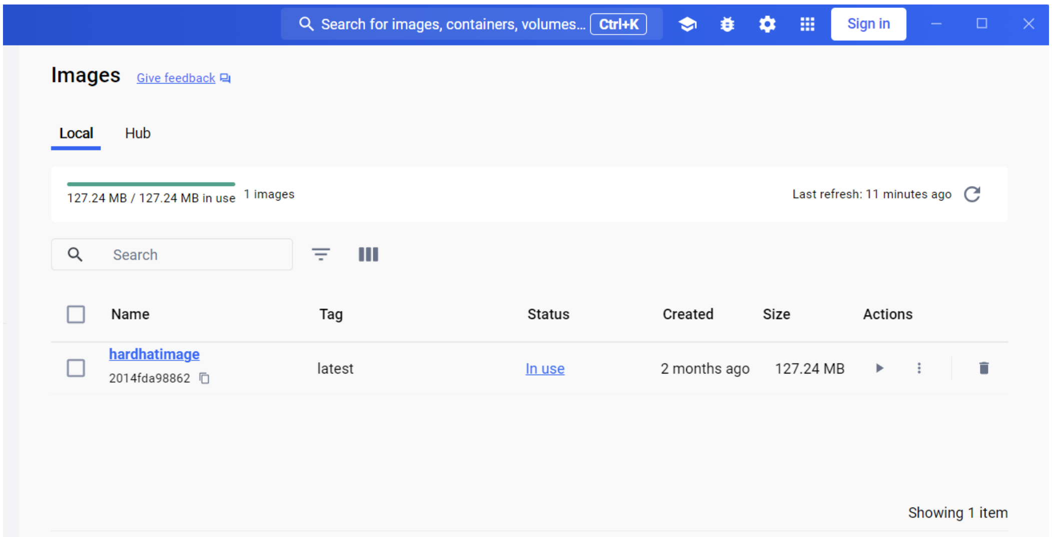


```
geth --networkid 14541 \
 --datadir ./node1 \
 --port 30301 \
 --http --http.addr=172.17.0.2 --http.port 8545 \
 --ws=true --ws.addr=172.17.0.2 --ws.port 8546 \
 --bootnodes enode://ad50e059b6ecabaedc447c2575443c2c58a310df294f2abc16dea45f300
 --unlock "0xea755EF8F3Bd7A39F1a1314875b3605e38c4214B" --password password.txt \
 --allow-insecure-unlock \
 --syncmode "full" \
 --ipcdisable \
 --mine=true \
 --miner.etherbase="0xea755EF8F3Bd7A39F1a1314875b3605e38c4214B" \
 console
```

Figure 4.4: Starting the nodes

4.2.4 Deploy in Docker

In figure4.5 Deploying a blockchain transaction in a Dockerized environment typically involves creating a containerized setup for interacting with a blockchain node.



127.24 MB / 127.24 MB in use 1 images

Last refresh: 11 minutes ago

Name	Tag	Status	Created	Size	Actions
□ hardhatimage 2014fda98862	latest	In use	2 months ago	127.24 MB	▶ ⋮

Figure 4.5: Docker deployment

4.3 Monero Initialization Transaction Broadcaster

In algorithm 4.1, solidity smart contract enables users to log Monero initialization transactions onto the Ethereum blockchain, providing a mechanism for secure and transparent cross-chain interactions. It bridges Monero's privacy features with Ethereum's immutability by recording transaction metadata, ensuring traceability and integration between the two ecosystems.

Algorithm 4.1 Monero Initialization Transaction Broadcaster

```
Input:
Ethereum sender address (msg.sender)
Monero transaction ID (_moneroTxId)
Monero public key (_moneroPublicKey)
Output:
Recorded Monero initializations in the array (initializations)
Event emitted for initialization broadcast (InitializationBroadcasted)
procedure BroadcastInitialization(_moneroTxId, _moneroPublicKey)
    Create a new MoneroInitialization record with:
    User: msg.sender
    MoneroTxId: _moneroTxId
    MoneroPublicKey: _moneroPublicKey
    Timestamp: block.timestamp
    Append the new record to initializations array.
    Emit the InitializationBroadcasted event with:
    User: msg.sender
    MoneroTxId: _moneroTxId
    MoneroPublicKey: _moneroPublicKey
    Timestamp: block.timestamp
end procedure
procedure GetInitialization(index)
    if index < initializations.length then
        Return the MoneroInitialization record at index, including:
        User address
        Monero transaction ID
        Monero public key
        Timestamp
    else
        Throw an error: "Invalid index"
    end if
end procedure
procedure GetInitializationCount
    Return the total count of initializations stored in the contract.
end procedure
```

4.4 Monero Transaction Logging

In algorithm 4.2, this feature enables the recording of Monero transaction metadata on the Ethereum blockchain, combining Monero's privacy with Ethereum's transparency.

Algorithm 4.2 Monero Transaction Logger

```
State Variables:
transactions: Array of MoneroTransaction structs
Struct: MoneroTransaction
Fields: user, moneroTxId, timestamp, notes
Event: TransactionLogged(user, moneroTxId, timestamp, notes)
procedure LOGTRANSACTION(_moneroTxId, _notes)
    Create MoneroTransaction with:
    user = msg.sender
    moneroTxId = _moneroTxId
    timestamp = block.timestamp
    notes = _notes
    Append MoneroTransaction to transactions
    Emit TransactionLogged
end procedure
procedure GETTRANSACTION(index)
    Require: index < transactions.length
    Return MoneroTransaction at transactions[index]
end procedure
procedure GETTRANSACTIONCOUNT
    Return transactions.length
end procedure
```

4.5 Monero Swap Smart Contract

In algorithm 4.3, this smart contract facilitates atomic swaps between Monero and Ethereum, enabling secure and trustless exchanges of assets across the two blockchains. It leverages Monero's privacy and Ethereum's transparency to ensure decentralized and verifiable transactions.

Algorithm 4.3 Monero Swap Smart Contract

```
State Variables:
swapCount: Total number of swaps recorded
swaps: Mapping of SwapRequest structs by ID
Struct: SwapRequest
Fields:
user: Ethereum address of the swap initiator
ethAmount: Amount of ETH sent
moneroAddress: Target Monero address
moneroTxId: Monero transaction ID (empty initially)
timestamp: Timestamp of the request
completed: Boolean indicating swap status
Events:
SwapInitiated(swapId, user, ethAmount, moneroAddress,
timestamp)
SwapCompleted(swapId, moneroTxId, timestamp)
procedure INITIATESWAP(_moneroAddress)
    Require: msg.value > 0
    Increment swapCount
    Create SwapRequest:
    user = msg.sender
    ethAmount = msg.value
    moneroAddress = _moneroAddress
    moneroTxId = ""
    timestamp = block.timestamp
    completed = false
    Store the SwapRequest in swaps[swapCount]
    Emit SwapInitiated
end procedure
procedure COMPLETESWAP(_swapId, _moneroTxId)
    Retrieve SwapRequest from swaps[_swapId]
    Require: !swap.completed
    Require: swap.moneroTxId == ""
    Update:
    swap.moneroTxId = _moneroTxId
    swap.completed = true
    Emit SwapCompleted
end procedure
procedure GETSWAP(_swapId)
    Return SwapRequest fields for swaps[_swapId]:
    user, ethAmount, moneroAddress, moneroTxId, timestamp,
completed
end procedure
procedure RECEIVE
    Revert with message "Use initiateSwap to send ETH"
end procedure
```

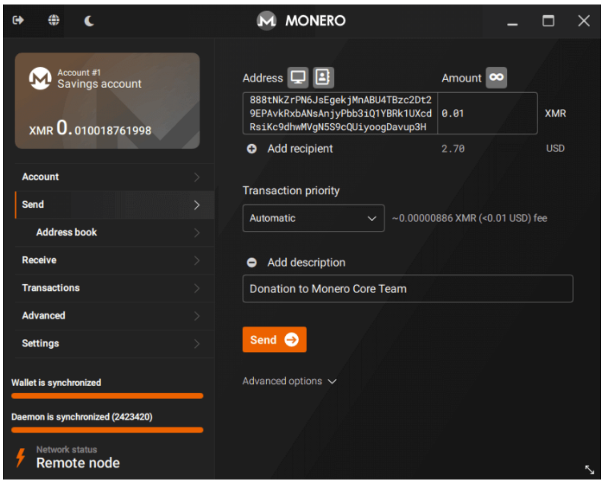
CHAPTER 5

RESULTS AND PERFORMANCE ANALYSIS

This chapter contains the results obtained and the related analysis with the related works carried out.

5.1 MONERO GUI

In figure.5.1 monero transaction, the sender generates a unique key image to prevent double-spending and constructs a ring signature using their private key along with a set of decoy public keys to ensure anonymity. The recipient's stealth address is derived, and the transaction amount is encrypted to maintain privacy. The sender then broadcasts the transaction to the network, where nodes validate the ring signature and confirm that the key image is unused. Once verified, the transaction is added to the blockchain, ensuring secure and private transfer of funds.



Account #1 Savings account

XMR 0.010018761998

Address: 888tNkZrPN6JsEgekjMnABU4TBzc2Dt2 9EPAvkRxbANsAnjyPbb3iQ1YBRk1UXcd RsiKc9dhwMVgN5S9cQUiyoogDavup3H

Amount: 0.01 XMR

2.70 USD

Transaction priority: Automatic

~0.00000886 XMR (<0.01 USD) fee

Add description: Donation to Monero Core Team

Wallet is synchronized

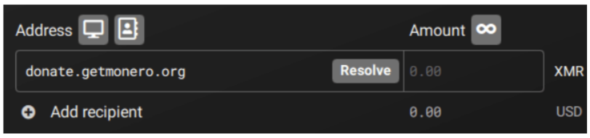
Daemon is synchronized (2423420)

Network status: Remote node

Figure 5.1: Monero GUI

5.2 MONERO TRANSACTION

In figure.5.2 addresses, which are human readable addresses (for instance, donate.getmonero.org). If you enter an OpenAlias address, a Resolve button will be displayed. Click on it to retrieve its Monero address.



donate.getmonero.org

0.00

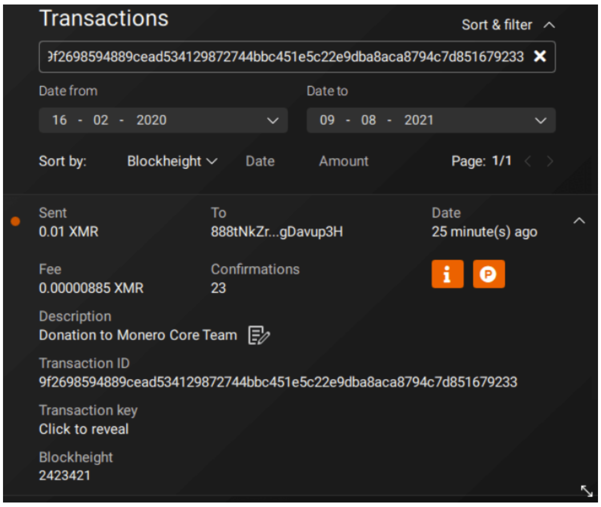
0.00

Figure 5.2: Transaction Address

5.3 TRANSACTION PAGE

In figure.5.3 the Transactions page allows you to see if your payment transaction was confirmed.There are three possible states for our sent transaction:

- Sent (Pending): The transaction has been sent to the Monero network but is awaiting confirmation by being included in a block by a miner. This process typically takes about 2 minutes but may take longer.
- Sent: The transaction has been successfully included in a block by a miner and is confirmed. The block number is displayed under ”Blockheight,” and the number of confirmations is shown under ”Confirmations.”
- Sent (Failed): The transaction could not be sent to the Monero network due to an issue. Refer to troubleshooting guidance to resolve the problem.



Transactions

Sort & filter

ɘf2698594889cead534129872744bbc451e5c22e9dba8aca8794c7d851679233 ✕

Date from: 16 - 02 - 2020

Date to: 09 - 08 - 2021

Sort by: Blockheight Date Amount Page: 1/1

Sent
0.01 XMR

To
888tNkZr...gDavup3H

Date
25 minute(s) ago

Fee
0.00000885 XMR

Confirmations
23

Description
Donation to Monero Core Team

Transaction ID
9f2698594889cead534129872744bbc451e5c22e9dba8aca8794c7d851679233

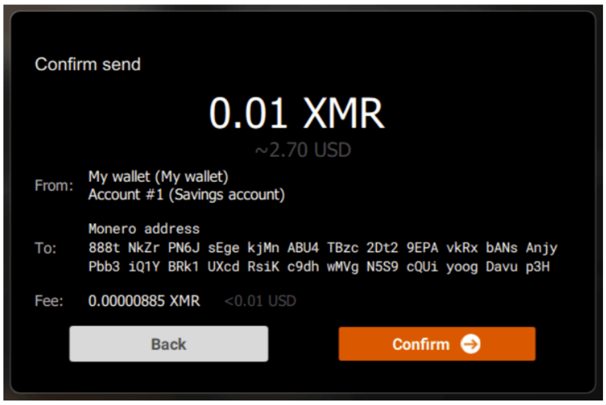
Transaction key
Click to reveal

Blockheight
2423421

Figure 5.3: Transaction Details

5.4 TRANSACTION CONFIRMATION

In figure.5.4 monero transaction confirmation involves validating and securely adding a transaction to the blockchain while maintaining privacy. After a transaction is broadcast, network nodes verify the ring signature to ensure the sender's ownership of the funds without revealing their identity. They also check the key image to confirm that it has not been previously used, preventing double-spending. Additionally, the nodes validate that the total input and output amounts are balanced, preserving confidentiality through encrypted values. Once these checks are successfully completed, the transaction is included in a block, and subsequent blocks built on top of it confirm its finality in the blockchain.



Confirm send

0.01 XMR

~2.70 USD

From: My wallet (My wallet)
Account #1 (Savings account)

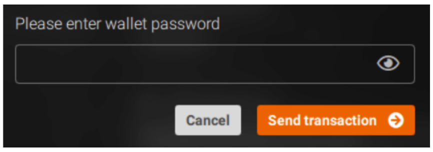
To: Monero address
888t NkZr PN6J sEge kjMn ABU4 TBzc 2Dt2 9EPA vkRx bANs Anjy
Pbb3 iQ1Y BRk1 UXcd RsiK c9dh wMVg N5S9 cQUi yoog Davu p3H

Fee: 0.00000885 XMR <0.01 USD

Figure 5.4: Confirmation

5.4.1 Wallet Confirmation

In figure.5.5 the user is prompted to enter their wallet password and click the ”Send Transaction” button to initiate the process.



Please enter wallet password

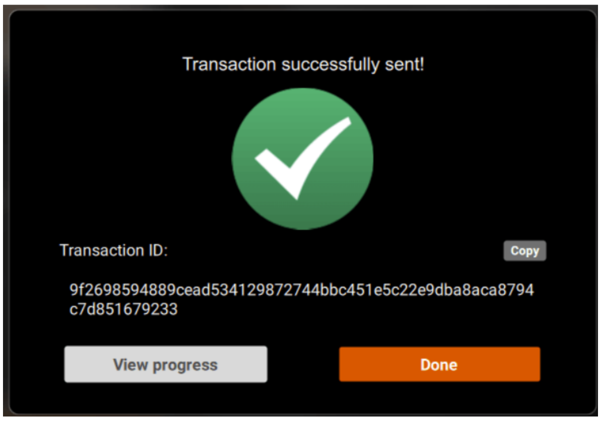
Figure 5.5: Wallet Confiramtion

5.5 TRANSACTION FINALIZATION

In figure.5.6 transaction is sent to the Monero network, it enters a pending state, waiting to be confirmed (included in a block) by a miner. This confirmation process typically takes around 2 minutes. Once the transaction is submitted to the network, there is no way to expedite the confirmation process.

The dialog displays the Transaction ID (txid), a unique identifier for the transaction. Users can click the ”Copy” button to copy the txid to the clipboard for reference. This ID can be entered on the Transactions page or block explorers to view transaction details. In some cases, recipients may request the transaction ID to verify receipt of the funds.

The ”View Progress” button directs users to the Transactions page, where they can monitor the blockchain and verify if the transaction has been confirmed.



Transaction successfully sent!

Transaction ID:

9f2698594889cead534129872744bbc451e5c22e9dba8aca8794
c7d851679233

Figure 5.6: Transaction Successful

5.6 PERFORMANCE ANALYSIS

To analyze the performance of main cost for Payer A lies in computing the accumulator and SoK in the Initialization and Swap Monero phases, while miners face costs during proof verification in the Swap Monero and Swap Bitcoin phases. A single round of Monero-Bitcoin exchange takes about 60.94 seconds, while tracing Payer A’s public key costs just 7.12 ms. Experiments indicate that the Swap Monero phase computation is nearly constant regardless of the number of input accounts, and increasing transactions per block (100–600) or cross-chain exchange proportions minimally affects proof generation and verification time. Even at maximum load, the verification time remains acceptable.

Phase	Payer A	Payer B	Miners	Tracing Authority
Initialization	341.10	2.20	15.80	0.79
Swap Mnero	150.33	-	3291.95	-
Swap Bitcoin	-	39.21	2249.49	-
Final Determination	-	-	3.30	-
Trace Monero	-	-	-	6.33

Table 5.1: COMPUTATION COST IN EACH PHASE

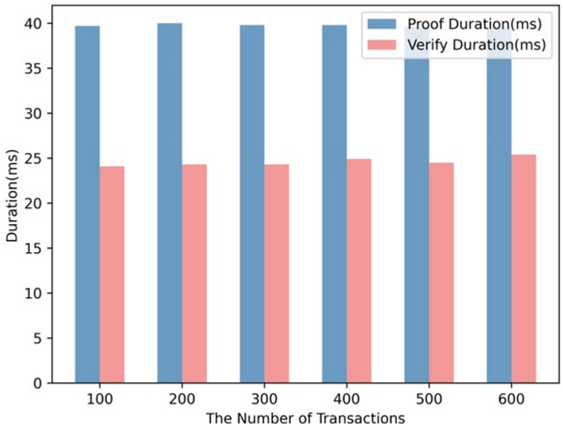


Figure 5.7: The impact of the number of transactions in each block for miners to verify the proof.

In figure.5.7 and figure.5.8 the graph shows the proof and verification durations (in milliseconds) for varying numbers of transactions, ranging from 100 to 600. Proof durations consistently hover around 40 ms across all transaction volumes. Verification durations are shorter, approximately 25 ms, and remain stable irrespective of the number of transactions. This indicates the computational cost for both processes scales efficiently. The proof duration is nearly double that of the verification duration.

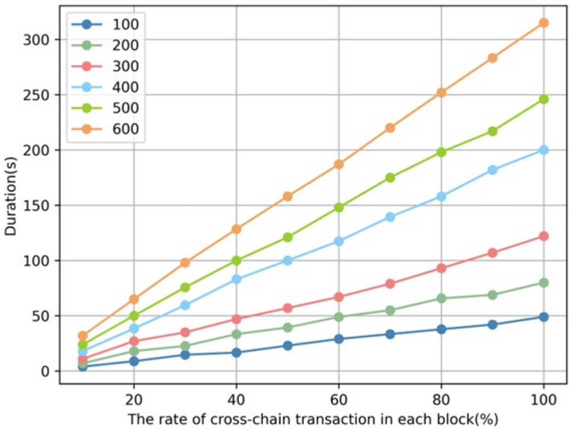


Figure 5.8: The verification time of miners with the proportion of transactions.

5.7 CHALLENGES IN IMPLEMENTATION

Implementing a privacy-preserving, policy-enforcement cross-chain transaction protocol faces several challenges. One of the primary difficulties is balancing user privacy with regulatory requirements, as the system must ensure user anonymity while allowing selective traceability for regulatory investigations. The cryptographic complexity involved, including the use of zero-knowledge proofs and signatures of knowledge, demands meticulous design to achieve both efficiency and security. Performance optimization is another hurdle, as the protocol must minimize latency and computational costs to ensure smooth transaction processing. Interoperability between heterogeneous blockchain systems, such as UTXO-based Bitcoin and privacy-centric Monero, adds to the complexity due to their differing structures. Scalability also poses a challenge, as the protocol needs to handle increasing transaction volumes while maintaining efficiency. Additionally, the system must defend against specific vulnerabilities, such as side-channel attacks, that could compromise user anonymity. Ensuring usability without requiring extensive modifications to existing blockchain systems or trusted hardware is crucial, as is addressing the burden on miners who must validate complex proofs. Finally, regulatory acceptance and trust in the system’s tracing mechanisms are essential for widespread adoption while safeguarding against malicious actors who may attempt to exploit the protocol for illegal activities. These challenges highlight the need for a well-rounded, secure, and efficient design to achieve the desired balance of privacy and regulation.

CHAPTER 6

CONCLUSION AND FUTUREWORK

6.1 CONCLUSION

The proposed protocol for privacy-preserving, policy-enforcement cross-chain transactions addresses critical challenges in ensuring secure and efficient interactions across heterogeneous blockchain systems. By leveraging advanced cryptographic techniques, such as zero-knowledge proofs and signatures of knowledge, the protocol ensures both privacy and traceability, enabling regulatory compliance without compromising user anonymity. Its scalability and interoperability make it suitable for diverse blockchain platforms, while efficient proof and verification processes highlight its practical viability. The system strengthens trust and security in cross-chain transactions, providing a robust foundation for modern decentralized ecosystems. This solution marks a significant advancement in privacy-focused, cross-chain blockchain interoperability.

6.2 FUTURE WORK

Future work in the development of the privacy-preserving, policy-enforcement cross-chain transaction protocol will focus on enhancing its scalability and efficiency to support higher transaction volumes without compromising security or performance. Further research will be conducted to improve interoperability with an even broader range of blockchain architectures, including emerging platforms and privacy-focused networks. Additionally, optimizing cryptographic operations to reduce proof and verification durations will be prioritized to ensure seamless adoption in real-world applications.

Another key area of future exploration will involve strengthening defenses against potential side-channel attacks and other adversarial threats to further safeguard user privacy and data integrity. Efforts will also focus on enhancing the usability of the protocol by simplifying integration with existing blockchain systems and minimizing technical complexities for users and developers.

Moreover, to foster broader adoption, future research will aim to incorporate more robust mechanisms for compliance with evolving regulatory frameworks, ensuring the protocol remains adaptable to global standards. Finally, pilot implementations and real-world testing will be undertaken to evaluate the protocol's effectiveness in diverse scenarios, providing valuable insights for continuous improvement and innovation.

REFERENCES

[1] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability. *Cryptology ePrint Archive*, 2018.

[2] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE symposium on security and privacy (SP)*. IEEE, 2018.

[3] Yuxian Li, Jian Weng, Ming Li, Wei Wu, Jiasi Weng, Jia-Nan Liu, and Shun Hu. Zerocross: A sidechain-based privacy-preserving cross-chain solution for monero. *Journal of Parallel and Distributed Computing*, 169, 2022.

[4] Tiancheng Xie, Jiaheng Zhang, Zerui Cheng, Fan Zhang, Yupeng Zhang, Yongzheng Jia, Dan Boneh, and Dawn Song. zkbridge: Trustless cross-chain bridges made practical. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022.

[5] Noether Shen. Ring signature confidential transactions for monero. *Tech. rep. Cryptology ePrint Archive, Report 2015/1098*, 2015.

[6] Alexei Zamyatin, Dominik Harz, Joshua Lind, Panayiotis Panayiotou, Arthur Gervais, and William Knottenbelt. Xclaim: Trustless, interoperable, cryptocurrency-backed assets. In *2019 IEEE symposium on security and privacy (SP)*. IEEE, 2019.

[7] Yanran Zhang, Sheng Hu, Qin Wang, Bo Qin, Qianhong Wu, and Wenchang Shi. Pxcrypto: A regulated privacy-preserving cross-chain transaction scheme. In *International Conference on Algorithms and Architectures for Parallel Processing*. Springer, 2022.

[8] Yuping Yan, George Shao, Dennis Song, Mason Song, and Yaochu Jin. He-dksap: Privacy-preserving stealth address protocol via additively homomorphic encryption. *arXiv preprint arXiv:2312.10698*, 2023.

[9] ZW Lei, Y Zhu, J Zhang, et al. Design of a supervised blockchain cross chain platform. *Computer & Digital Engineering*, 49(12):2544–2550+, 2021.

[10] Sri AravindaKrishnan Thyagarajan, Giulio Malavolta, and Pedro Moreno-Sanchez. Universal atomic swaps: Secure exchange of coins across all blockchains. In *2022 IEEE symposium on security and privacy (SP)*. IEEE, 2022.

[11] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Satoshi Nakamoto*, 2008.

[12] Gavin Wood. Polkadot: Vision for a heterogeneous multi-chain framework. *White paper*, 21, 2016.

[13] Iddo Bentov, Yan Ji, Fan Zhang, Lorenz Breidenbach, Philip Daian, and Ari Juels. Tesseract: Real-time cryptocurrency exchange using trusted hardware. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 2019.

[14] Goshgar Ismayilov and Can Özturan. Ptts: Zero-knowledge proof-based private token transfer system on ethereum blockchain and its network flow based balance range privacy attack analysis. *Journal of Network and Computer Applications*, 233, 2025.

[15] Elli Androulaki, Angelo De Caro, Kaoutar Elkhiyaoui, Christian Gorenflo, Alessandro Sorniotti, and Marko Vukolic. Multi-shard private transactions for permissioned blockchains. *arXiv preprint arXiv:2010.08274*, 2020.

[16] Gary Yu. Blockchain stealth address schemes. *Cryptology ePrint Archive*, 2020.

[17] Jae Kwon and Ethan Buchman. Cosmos whitepaper. *A Netw. Distrib. Ledgers*, 27, 2019.

[18] Jiasi Weng, Jian Weng, Jilian Zhang, Ming Li, Yue Zhang, and Weiqi Luo. Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing*, 18, 2019.

[19] Florian Tramèr, Dan Boneh, and Kenny Paterson. Remote {Side-Channel} attacks on anonymous transactions. In *29th USENIX security symposium (USENIX security 20)*, 2020.

[20] Yuwei Xu, Ran He, Shengjiang Dai, and Yujian Zhang. Chainkeeper: A cross-chain scheme for governing the chain by chain. *IET Blockchain*, 3, 2023.