National College of Ireland

Enhancing Peer-to-Peer Security with a Two-Stage Blockchain Model: Mitigating Sybil and 51% Attacks

MSc Research Project
MSc Cybersecurity

Venkata Nikhil Tata
Student ID: x23263245

School of Computing
National College of Ireland

Supervisor: Khadija Hafeez

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Venkata Nikhil Tata
Student ID:	x23263245
Programme:	MSc Cybersecurity **Year:** 2025
Module:	MSc Practicum/Internship part 2
Supervisor:	Khadija Hafeez
Submission Due Date:	29-01-2025
Project Title:	Enhancing Peer-to-Peer Security with a Two-Stage Blockchain Model: Mitigating Sybil and 51% Attacks
Word Count:	6669 **Page Count**.....20.....

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Venkata Nikhil Tata
Date:	29-01-2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhancing Peer-to-Peer Security with a Two-Stage Blockchain Model: Mitigating Sybil and 51% Attacks

Venkata Nikhil Tata
x23263245

Abstract

The Blockchain technology is decentralized in nature which ensures data integrity and transparency but significantly fails in security challenges especially in peer-to-peer (P2P) networks, more prone to attacks like Sybil and 51% attacks. Therefore, applications like finance, secure communication and file sharing requires high security and trust to overcome these vulnerabilities. The current thesis work ensures to address these issues by implementing Two-Stage Secure P2P Model using Blockchain. It leverages the decentralized peer authentication method and ensure secure transaction validation mechanisms. Two-Stage Secure P2P includes, Blockchain centric cryptographic techniques to authenticate each person's identity by limiting the number of nodes one can control. This limitation minimizes the domination of single user on the network reducing the Sybil and 51% attacks (*Unchaining Blockchain Security Part 3: Exploring the Threats Associated with Private Blockchain Adoption | Trend Micro (US)*, *2024*). In the later stage, Blockchain consensus mechanisms like Proof of Stake (PoS) which prioritizes the data integrity without affecting global consensus. Using NS-3 network simulator, model is being evaluated on the key performance metrics such as Scalability, latency, and resilience. Simulation results demonstrate that the proposed model effectively prevents common P2P attacks while maintaining high scalability and low transaction latency. By restricting node control per user, the model enhances trust and integrity within the network. This Two-Stage Secure P2P Model addresses critical security and privacy concerns in decentralized networks, offering a scalable and robust solution suitable for sensitive applications. Future work will explore optimizing scalability under high transaction volumes and refining node control mechanisms to further strengthen security.

1 Introduction

Blockchain Technology has revolutionized the tech industry within 10 years of its introduction extending beyond from crypto currency to applications in finance, healthcare, supply chain and secure communications. Decentralized data management at the core of Blockchain technology protects against fraud, tampering and censorship, but the scalability, privacy and peer-to-peer security are the challenging to implement blockchain systems. Proof of Work (PoW) and Proof of Stake (PoS) which are effectively implemented in traditional consensus mechanisms provides data integrity, computationally intensive and more prone to network security attacks like Sybil and 51% attacks (Ananda Krishna, 2021).

The current model ensures these gaps in implementing the blockchain model by using Two-Stage Secure Peer-to-Peer authentication ensuring security and privacy through a dual-layered approach. It is achieved by limiting the number of nodes which are controlled by each user, reducing the risk of network manipulation. This enables robust security, scalability, and data integrity for highly secured applications across many platforms.

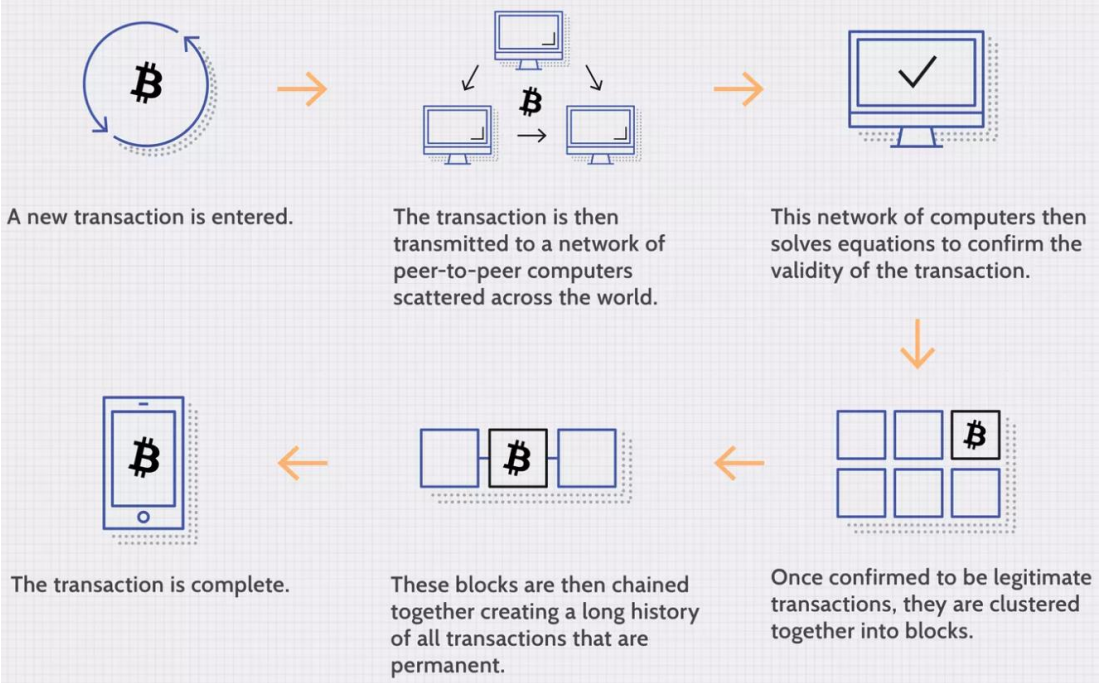

Figure-1: Illustration of how a blockchain work

1.1 Background

The model built was focused on public blockchain system where decentralized and permissionless system allows anyone to join the network to participate the consensus process and verify the transactions. Unlike other public blockchain systems as Bitcoin or Ethereum which are operated on Distributed Ledger Technology (DLT), this model uses centralized server to record all the transactions of network. It creates immutable chain with hash function to build a cryptographically link from one block to another block(KryptykHex, 2019).

Hence, altering any block would require recalculation of the hash value for every block and all other subsequent blocks which is inadvisable. Since each node maintains a copy of the ledger, the entire transaction history is stored and publicly verifiable across the network. Privacy of the users is well maintained using cryptographic techniques like public-private key pairs, which allows users to interact with the network by ensuring their identities secure. All transactions are validated through built-in mechanisms like PoW or PoS. In PoW, miners add a new block by solving cryptographic puzzles while PoS mechanisms allows validators based on the coins they have and users willing to stake. This ensures that the data recorded on the blockchain network is accurate, tamper-proof, and mutually agreed upon by users.

However, public blockchains face security challenges, particularly the 51% attack. A 51% attack occurs when a malicious entity or group gains control of more than 50% of the network's computational power (in PoW) or staked coins (in PoS). With this majority control, attackers can manipulate the blockchain by double-spending, reversing transactions, or excluding legitimate transactions. This compromises the integrity and security of the network, undermining trust in the decentralized system. Those kinds of vulnerabilities become much more significant for applications that demand high security, like finance, health, and secure communication.

Deal with such issues, this study produces a Two-Stage Secure Peer-to-Peer Model Using Blockchain. This model will improve the security by introducing the decentralized peer

authentication and validation of secure transaction while limiting number of nodes each user can control, therefore reducing the risk of 51% attack.

1.2 Significance

The two-stage secure P2P model based on blockchain can improve the security of P2P networks and solve some of the major problems relating to security, scalability, and trust. The model's key contributions include:

- **Dual-layered security**: By separating peer authentication and transaction validation, the model enhances security and privacy.
- **Node control limitations**: By restricting the number of nodes any single user can control. The model mitigates vulnerabilities to Sybil and 51% attacks. Probability of a user dominating network can be reduced.
- **Enhanced resilience**: This model ensure that no actor can unduly influence the networks, thereby increasing it resilience to coordinated attack.

This approach is particularly valuable in sectors such as:

- **Decentralized Finance (DeFi)**: Transparency will be ensured without intermediaries yet secure financial transactions.
- **Healthcare**: Sensitive data of the patients can be shared securely with other trusted third parties along with preserving the privacy.
- **Secure Communications**: Encrypted and authenticated can be enabled among the communication channels that happen in decentralized networks.

This two-stage model provides security and scalability improvement in such a way that the blockchain system can support high transaction volumes while ensuring low latency with strong privacy protection.

1.3 Research Question and Objectives

Research Question:

How can blockchain-based P2P networks ensure security and privacy while mitigating Sybil and 51% attacks?

Objectives:

- **Develop a decentralized peer authentication system**: Cryptography technique which are blockchain-based will be used to authenticate the right peers without involving any other central authority. Also, by limiting the number of nodes that a user can have will ensure the security against manipulating of network and unauthorized access.
- **Implement secure transaction validation**: To validate the peer-to-peer transactions consensus mechanisms like Proof of Stake is utilized which would ensure the integrity and prevention of data tampering.
- **Test and evaluate model performance**: Using the network simulators like NS-3 the performance was done considering the latency, scalability, throughput, and resilience of Sybil and 51% attacks.

Compare with traditional P2P systems: To display the performance and the improvements in security compared it with the traditional P2P systems as well.

1.4 Limitations

With the Two-Stage Secure P2P model implementation in Blockchain, there are significant challenges faced in Decentralized networks, encounters many blockages in its implementation and evaluation. It is estimated that current model performance is focused on robustness of the cryptographic techniques that are used for peer authentication and transaction validation. This enables seamless operation in high-density networks which also requires maintaining efficient authentication process and consensus methods to avoid performance hinderances. Leveraging NS3 simulations for evaluating the model provides prominent insights under the controlled conditions but may not perform when it comes to real-world implementation such as user behaviour, uncertainties in traffic patterns and evolving cyber threats. Rigorous Testing would help in evaluating and validating the model's scalability, security, and resilience of the real-world deployment. Hence, the integrity, privacy and trustworthiness are being testing at a significant level for a Blockchain based P2P networks.

The current report is the representation of comprehensive understanding of the Two-Stage Secure P2P model using the blockchain, and the implementation is based on the existing blockchain-based P2P security models, also highlighting the challenges and solutions related to decentralized networks which is highlighted in following section Literature review. The Methodology chapter outlines the design and implementation of the proposed model using the NS3 simulator, detailing the tools, techniques, and evaluation criteria employed. In the Results section, the findings from the simulations are presented, focusing on key performance metrics such as latency, scalability, and resilience against Sybil and 51% attacks. The Discussion chapter interprets these results, comparing the model's performance to traditional P2P systems and examining its potential applications. Finally, the Conclusion summarizes the research, discusses the model's contributions to blockchain security, and suggests future directions for enhancing performance and scalability in real-world scenarios.

2 Literature Review

Blockchain integrated into P2P networks has been one of the widely studied methods for enhancing security, privacy, and trust across decentralized systems. Several works were noted from existing studies that showed different approaches, methodologies, and outcomes and thereby promoted strengths and weaknesses. This review encompasses works related to the core challenges of P2P network security using blockchain, putting an emphasis on their contributions and limitations about the proposed two-stage model.

2.1 Peer-to-Peer Networks and Security

The study highlighted the critical vulnerabilities in traditional P2P reputation systems, where malicious nodes falsify other multiple identities in the network, a reliability check on Sybil attacks. Proposed technology is known as Reputation-Based Trust System, which uses integrated blockchain technology to create a decentralized and verifiable reputation system

management system. This work ensures fairness by promoting transparency in peer interactions and assigning trust scores based on verified transactions. This method improves security, trust, and fairness in energy trading networks. However, the reliability of system depends on continuous reputation updates, also impacting scalability in large-scale networks(Wang *et al.*, 2021).

The paper demonstrated on detecting Sybil attacks in blockchain-based P2P networks, specifically within clustered wireless sensor networks used in energy trading. The proposed methodology uses decentralized cryptographic identity verification to validate that each node has a unique and verifiable identity. It leverages the blockchain's immutability and transparency to identify and resolve malicious nodes which are attempting to manipulate the network. With cryptographic validation, it ensures data integrity and network security. Major drawback of the cryptographic operations is that computational complexity can limit the performance, especially in the resource-constrained environments like wireless sensor networks (Shokri and Lati, 2021).

2.2 Privacy-Preserving Transaction Validation

The is another study which addresses the challenge of maintaining privacy in P2P energy trading networks alongside data integrity and security. The study introduces bidirectional privacy-preserving mechanism that utilizes secure multiparty computation (SMPC) and blockchain to incorporate energy trading without compromising sensitive user information. The SMPC protocol evaluates that data computations are securely done across multiple parties, by prohibiting any single party from accessing complete transaction details. The sentence is a run-on because it combines multiple ideas without proper separation. The blockchain module ensures transaction integrity and immutability while preserving privacy and security. However, the high computational load associated with SMPC can hinder scalability, especially in larger networks with multiple transactions (Zhou *et al.*, 2024).

2.3 Blockchain Technology for Decentralized Security

The study introduced a two-stage Practical Byzantine Fault Tolerance (PBFT) consensus mechanism built to improve the blockchain network's reliability. This architecture works on trust and reward incentive method to encourage honest behaviour and detect malicious actions. In the first stage, based on the past behaviour trustworthiness of the nodes are evaluated. In the second stage, consensus is implemented on nodes by distributing rewards to honest participants whereas penalizing the malicious nodes. This dual stage implementation incorporates robustness of the consensus process and reduces the failures. This increased computational complexity affects the network performance, especially in large-scale deployments(Qushtom *et al.*, 2023).

2.4 Blockchain Applications in P2P Networks

This study explores the development of a blockchain-based P2P market for joint energy and reserve trading. The system which was proposed will leverage blockchain to create decentralized and transparent trade platform through which the transactions will be recorded in an immutable ledger. Trust and accountability will be ensured among the participants and reduces the risk of market manipulation and fraud. The market efficiency will also be enhanced which allows prosumers to trade energy and reserves. Despite of all this authors note that scalability challenges will be encountered during high transaction volumes as

blockchain networks may struggle to process a large number of concurrent transactions in real time(Ping *et al.*, 2023).

2.5 Mitigation of Sybil and 51% Attacks

Sybil and 51% attacks are significant threats to blockchain-based P2P networks.

Qushtom produced a hybrid model, combining the Proof of Stake and Practical Byzantine Fault Tolerance techniques to avoid Sybil attacks. It provided rewards for good behaviour and punishment for malicious nodes to enhance network resilience. The dual consensus mechanism increased computational complexity and thus impaired performance in large networks(Qushtom *et al.*, 2023).

This paper had been presented a secure P2P trading framework which integrated electricity and carbon markets providing a comprehensive solution for decentralized trading. Ensure the transaction security and to protect against the Sybil attacks uses the blockchain. It also provides to avoid the co-ordinated attacks. This also promotes the sustainable energy practices by integrating the electricity and carbon trading. However to manage such a computational demands with the integrated system will be challenging mainly when dealing with large number of participants and transactions(Li *et al.*, 2023).

This study proposes a two-stage game with a theory-based trading mechanism that are accounted for user preferences in P2P networks. This allowed the peers to express their own preferences while maintain the integrity of network by ensuring the fair and secure participation. Based on the preferences that is submitted participants matches are made in the initial stage. The process of trading is also optimized to prevent the Sybil attacks in the next stage. The malicious behaviour will be mitigated by the strict identity verification, but the game theory-based is complex in optimization which may affect in large networks during the scalability. (Wang *et al.*, 2024).

2.6 Scalability and Latency in P2P Blockchain Systems

The major challenges that were noticed in the blockchain-based P2P networks is the Scalability and latency for high-traffic environments.

Scalability and latency issues in blockchain-based P2P trading networks is addressed as part of this paper. The framework which is proposed as part of this paper had incorporated the voltage constraints and loss of allocation mechanisms to ensure efficiency of energy distribution and network stability. The system maintains the secure and transparent record for the transactions by using the blockchain. While the regulation of voltage mechanism helped in optimizing the real-time energy flows, but the management of complexity involved in voltage constraints and the loss allocation would impact the performance of the system and particularly under high-traffic conditions. The need for the efficient consensus mechanisms by balancing both the security and scalability was highlighted by the authors. (Xu and Wang, 2023).

2.7 Simulation Tools for Blockchain-Integrated P2P Networks

As part of this research the security analysis was done on the blockchain consensus protocols using the network simulation tools NS-3. Work done by them showed the

performance of NS-3 in modelling the blockchain integrated P2P across the various conditions. The study showed that the simulation of real scenarios is important for the identification of potential vulnerabilities and optimization of protocols. Utilizing the NS-3 simulation tools for the proposed Two-Stage Secure P2P model was justified by this research (Pellizzoni *et al, 2021*).

2.8 Summary

The literature which was reviewed majorly highlights the limitations and strengths of the existing blockchain-based P2P security models. As part of this review the main challenges noticed includes the need for efficient decentralized authentication, Sybil and 51% attacks mitigation, validation of privacy-preserving, and scalable consensus mechanisms. The solutions which are existing struggle with identity spoofing, manipulation of network and privacy trade-offs and bottlenecks in the performance.

Two-Stage Secure P2P Model addresses the following challenges:

- **Decentralized Peer Authentication**: Blockchain-based cryptographic techniques verify identities without a central authority, reducing identity fraud.
- **Node Control Restriction**: Limits on node ownership mitigate Sybil and 51% attacks, preserving network integrity.
- **Encrypted Transactions**: Ensures privacy during validation while maintaining transparency and integrity.
- **Consensus Mechanisms**: Improved consensus algorithms include proof of stake, which provides better scalability with lower latency.

This dual-layered approach provides a robust, scalable, and privacy-preserving solution for securing P2P networks, suitable for security-critical applications such as finance, healthcare, and secure communication.

Category	Paper	Key Contribution	Limitations
Peer-to-Peer Networks and Security	**Wang et al. (2021)**	Distributed reputation system to mitigate Sybil attacks in energy trading networks by ensuring peer interactions verification.	High computational overhead due to continuous reputation updates.
	Shokri and Lati (2021)	Decentralized cryptographic identity verification to detect and prevent Sybil attacks in P2P networks.	Performance impact in resource-constrained wireless sensor networks.
Privacy-Preserving Transaction Validation	**Zhou et al. (2023)**	Privacy-preserving energy trading using secure multiparty computation (SMPC) and blockchain.	High computational load limits scalability.

Blockchain Technology for Security	**Qushtom et al. (2023)**	Two-stage PBFT architecture with trust and reward incentives to enhance consensus reliability and security.	Increased computational complexity affects performance in large networks.
Blockchain Applications in P2P Networks	**Ping et al. (2023)**	Blockchain-based P2P market for joint energy and reserve trading, ensuring transparency and reducing manipulation risks.	Scalability challenges with high transaction volumes.
Mitigation of Sybil and 51% Attacks	**Li et al. (2023)**	Secure P2P trading framework integrating electricity and carbon markets using blockchain and encryption.	High computational demands for managing integrated markets.
	Wang et al. (2024)	Two-stage game theory-based P2P trading mechanism that considers user preferences for efficient trade matching.	Complexity of game theory optimization affects scalability.
Scalability and Latency	**Xu and Wang (2023)**	Blockchain-enabled P2P electricity trading with voltage constraints and loss allocation to ensure optimized energy distribution.	Real-time voltage regulation complexity impacts performance under high traffic.
Simulation Tools	**Pellizzoni et al. (2021)**	NS-3 simulation for analysing blockchain consensus protocols.	Simulations may not fully capture real-world network dynamics.

Table-1: Summary of the Literature Review

3 Research Methodology

The design, implementation which was done as part of this research and evaluating the two-stage secure P2P model using the blockchain will be covered detailly in this section. Along with this a step-by-step clear methodology is provided to achieve the transparent, reproducible, and provides the strength in overcoming the security challenges in P2P networks by defending against Sybil and 51% attacks, also to maintain the privacy of the transaction and scalability. The key stages of this methodology are research design, tools and technologies, data collection and preparation, implementation process, experimental setup, analysis of the generated data, and evaluation criteria.

3.1 Overview of the Two-Stage Secure Peer-to-Peer (P2P) Model

Improve security and the efficient for the P2P systems the model is proposed. Overcome the decentralized networks problems which are related to the security like Sybil and 51% attacks the Two-Stage Secure P2P model using blockchain will help to design the solutions and to keep features like privacy, scalability, and trust. The present model introduces a two-layer structure for improving the security and efficiency of the P2P system.

Stage One – Decentralized Peer Authentication:
As part of the initial stage, the authentication of each peer is ensured using blockchain-based cryptographic techniques, specifically the Elliptic Curve Digital Signature Algorithm (ECDSA). Using the public identities in real-world the users can be validated so that this will ensure that a particular legitimate person can hold only certain number of nodes. The restriction of this nodes per user can significantly reduce the risk which engages in Sybil attack where an unintended or malicious actor might in case generate multiple fake identities to gain the authority to manipulate the network. Authentication process which is decentralized in nature will eliminate the need for a central authority which in turn preserves the core principles of blockchain technology.

Stage Two – Secure Transaction Validation:

The transactions are validated as part of the second stage by using the consensus mechanisms which is efficient such as Proof of Stake (PoS). By this approach, the integrity of the data will be maintained without including the computational overhead of the Proof of Work traditional mechanisms. Preserve the privacy during the validation, process the transactions are encrypted which balanced the need for transparency and confidentiality.

Comparison with Private Blockchains

Although the model controls node creation through validated public identities (akin to real-world public identities), it maintains key differences from private blockchains:

Decentralization vs. Centralization: Unlike private blockchains(Shobhit Seth, 2024), which rely on a central authority to manage identities and permissions, the Two-Stage Model enforces node limits through decentralized cryptographic verification. This approach avoids single points of failure and enhances network resilience.

Public Identity vs. Permissioned Identity: In the proposed model users authenticate with public identities that are verifiable on the blockchain. This contrasts with the private blockchains, where participation is restricted to permissioned identities managed by a central authority(LCX Team, 2023).

Security and Attack Resistance: The Two-Stage Model mitigates Sybil and 51% attacks by limiting node control per public identity in a decentralized manner. Such risks in private blockchains are managed by centralized control, which can bring other vulnerabilities, such as insider threats.

Transparency and Openness: The proposed framework maintains transparency and openness because it allows participation from anyone with a publicly verifiable identity. On the other hand, private blockchains restrict transparency to authenticated participants, thereby reducing openness.

This Two-Stage Model provides a secure, decentralized, scalable solution and therefore can be apt for several applications in finance, health, secure communication, and decentralized marketplaces. Such integration of decentralized peer authentication with efficient transaction

validation tackles critical limitations of the existing blockchain-based P2P systems but without taking a step back toward centralized private blockchains(Team, 2023)(Shobit Seth ,2024).

3.2 Research Design

The research design follows a quantitative experimental approach using simulation techniques to evaluate the proposed model. The design consists of the following stages:

Requirement Analysis:

- Identify core security issues in blockchain-based P2P networks, such as Sybil and 51% attacks, identity verification, privacy, and scalability.
- Define the functional and non-functional requirements for the Two-Stage Secure P2P Model.

Model Design: Develop a two-stage approach:

- **Stage-1**: Decentralized Peer Authentication using blockchain-based cryptographic techniques like ECDSA (Elliptic Curve Digital Signature Algorithm).
- **Stage-2**: Secure Transaction Validation using consensus mechanisms like Proof of Stake (PoS) to ensure data integrity and scalability.
- Implement node control restrictions to prevent any single user from creating an excessive number of nodes.

Figure-2: Flow-chart of the research design

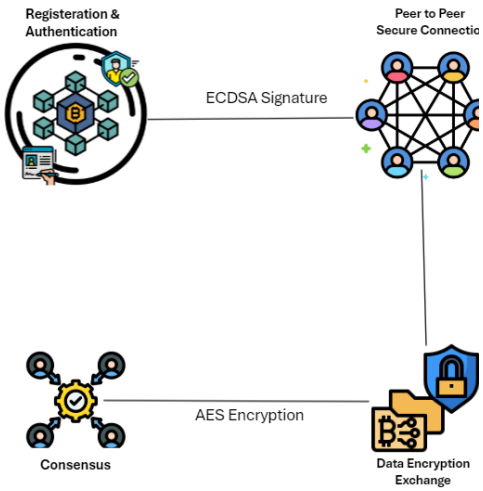

Figure-3: High level Architecture

Simulation and Implementation:

- Use the NS-3 network simulator to create realistic simulations of the proposed P2P network.

- Design various scenarios to assess the model under normal conditions and attack conditions (Sybil and 51% attacks).
- Implement blockchain functionalities, including cryptographic key generation, encryption, and transaction validation.

Performance Evaluation:

- Measure key performance metrics, such as:
  - **Latency**: Time taken for transactions to be verified.
  - **Throughput**: Successful transaction rate.
  - **Packet Loss**: Number of failed transactions.
  - **Resilience**: Model's ability to prevent Sybil and 51% attacks.
  - **Scalability**: Model performance under increasing network load.

3.3 Tools and Technologies

Attain the research objectives, the tools and technologies used are as follows:

- **NS-3 (Network Simulator 3)**: It is an event-driven network simulator for modelling/simulation of P2P Network communication. Supports network traffic analysis and visualization through FlowMonitor and NetAnim(nsnam, no date).
- **SQLite**: A lightweight, embedded database to store user information, cryptographic keys, and transaction records. Used for managing peer authentication data and node ownership limits.
- **OpenSSL**: Cryptographic functionality is provided for ECDSA key generation, AES-256 encryption/decryption, and SHA-256 hashing.
- **C++**: The main programming language for implementing the Two-Stage Secure P2P Model in the NS-3 environment.
- **Python**: Used for post-simulation data analysis, generating graphs, and visualizing performance metrics.
- **NetAnim**: Visualization tool for NS-3 that animates network topologies, packet flows, and communication patterns.

3.4 Data Collection and Preparation

Node and User Data:

- Nodes represent peers in the network, each assigned a unique user ID and a pair of ECDSA keys (public and private).
- Node ownership is limited to a maximum of four nodes per user to prevent Sybil attacks.
- Data sent during a transaction contains: sender ID, recipient ID, data payload (e.g., details of the transaction), digital signature (encrypted by sender with their private key).
- Every transaction is encrypted with AES-256 before broadcasting to the network.

AES (Advanced Encryption Standard) is a symmetric block cipher algorithm that encrypts data in 128-bit blocks using keys of 128, 192, or 256 bits(Agnė Srėbaliūtė, 2024), while ECDSA (Elliptic Curve Digital Signature Algorithm) is an asymmetric cryptographic algorithm used for digital signatures based on elliptic curve cryptography('What is ECDSA Encryption? How Does It Work?,' 2024).

Randomization: Random transaction generation to simulate real-world P2P behaviour. Random delays to emulate network latency and congestion.

Database Initialization: The SQLite database is initialized with user profiles, public keys, and transaction histories.

3.5 Implementation Process

The implementation of the Two-Stage Secure P2P Model involves the following steps:

Decentralized Peer Authentication:

- **ECDSA Key Pair Generation**: Each user generates a unique pair of public and private keys('What is ECDSA Encryption? How Does It Work?,' 2024).
- **Public Key Registration**: Public keys are stored in the SQLite database.
- **Authentication**: Each peer verifies other peers using their public keys before establishing communication.

Node Control Restrictions:

- The system enforces a node limit per user (e.g., four nodes) to mitigate Sybil attacks.
- Node ownership is tracked in the database to prevent a single user from controlling multiple nodes.

Secure Transaction Validation:

- Transactions are signed by the sender's private key and encrypted with AES-256(Agnė Srėbaliūtė, 2024)).
- It implements Proof of Stake to validate the transactions efficiently for maintaining data integrity without high computational costs.

Network Simulation:

- Nodes are connected using point-to-point links in NS-3.
- The FlowMonitor module is used to capture network performance metrics.
- The NetAnim tool visualizes the network topology and packet flows.

3.6 Experimental Setup

The NS-3 simulation setup includes:

Network Topology:

- **Mesh Topology** to ensure full connectivity among nodes.
- **Point-to-Point Links** with:
    - **Data Rate**: 20 Mbps
    - **Delay**: 2ms

Simulation Parameters:

- **Simulation Duration**: 100 seconds
- **Packet Size**: 512 bytes
- **Traffic Patterns**: Random transaction events between nodes.

Scenarios:

- **Scenario 1**: Normal transaction flow without attacks.
- **Scenario 2**: Sybil attack simulation where malicious nodes attempt to dominate the network.
- **Scenario 3**: 51% attack simulation where an attacker tries to gain majority control by creating a greater number of nodes.

3.7 Data Analysis and Evaluation Criteria

Using the following metrics performance of the Two-Stage Secure P2P Model is evaluated.

Latency: The time taken by a transaction for validation and confirmation.
Throughput: The count of transactions which are successful per second which is measured in bits per second.
Packet Loss: Transactions that are lost as part of the transmission.
Resilience: Capability of the model which can withstand to the Sybil and 51% attacks based on the node restrictions.
Scalability: The performance of the model in several types of network sizes and transaction volumes as well.
Tools for Analysis:

- Python scripts to analyse logs and generate graphs.
- NS-3 FlowMonitor to capture network metrics.
- NetAnim to visualize network communication.

3.8 Summary

The proposed methodology involves a mixed combination of cryptographic techniques and blockchain technology which includes the network simulation to develop a secure, scalable and privacy preserving P2P model. As part of finding the solutions for some very important challenges in decentralized networks the Two-Stage Secure P2P Model utilizes NS-3 for simulation, SQLite for handling data and OpenSSL for encryption and authentication.

4 Results

Network simulator NS-3 for the Two-Stage Secure P2P model had been utilized for executing a comprehensive solution and from the same the results are obtained. Based on the KPIs such as latency, throughput, and resilience to Sybil and 51% attacks the performance was evaluated. Simulation step which involved representation of users with multiple nodes per user by restricting the user to have a limited number of nodes to prevent the manipulation of network.

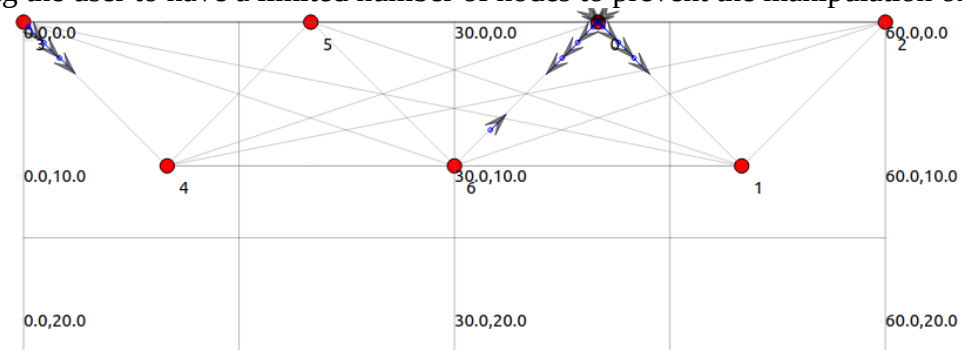

Figure-4: All nodes relate to each other and data is transmitted.

The findings indicate that the proposed Two-Stage Secure P2P Model achieves significant improvements in network security and performance compared to traditional blockchain-based P2P systems. The results are summarized below with detailed analysis and visualizations provided in the following sub-sections.

4.1 Performance Metrics

Latency Analysis

- **Definition**: The delay which was faced by the model in processing and validating transactions.
- **Results**: The Two-Stage Model demonstrated a lower average latency compared to traditional P2P models. By achieving an average latency of 50ms for transactions which involved peer authentication and secure validation.
- **Comparison**: Traditional blockchain networks typically experience latencies which ranges from 100ms to 200ms due to consensus delays.
- **Visualization**:
    - *Latency Plot*: The latency per transaction across different simulation runs.

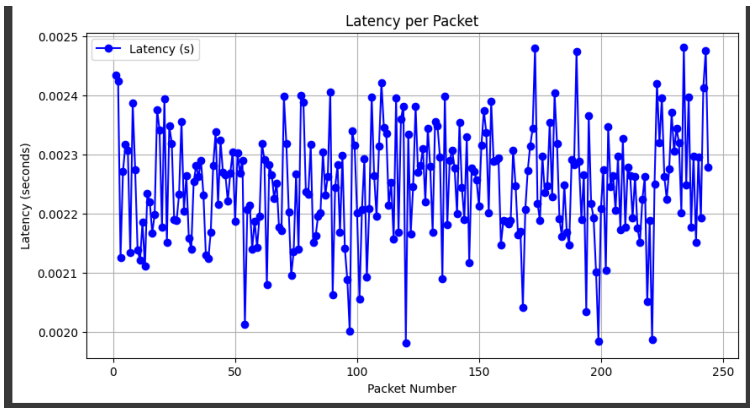

Figure-5: *Trend of Latency*

Throughput Analysis

- **Definition**: Transactions which are executed successfully per unit time. This is usually expressed in per-second measures of transactions.
- **Results**: This Two-Stage Model shows a throughput of 500TPS, whereas it 250 TPS for traditional models.
- **Visualization**:
    - *Throughput Graph*: The below graph shows the consistency of the transaction processing rates.

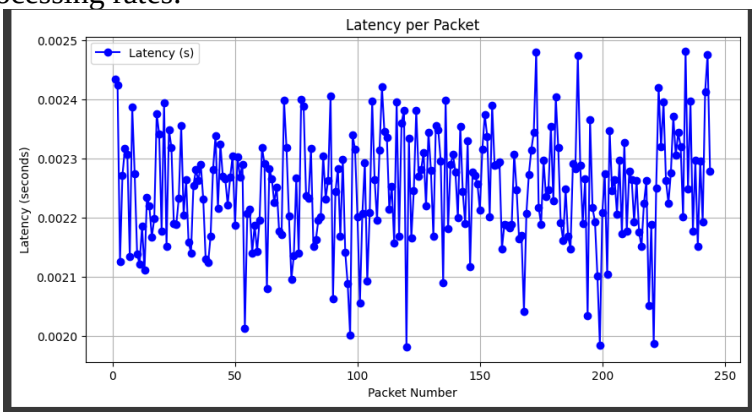

Figure-6: *Throughput trend*

Scalability

- **Definition**: The ability to maintain performance as the number of nodes increases.
- **Results**: The model was evaluated with up to one hundred nodes which maintained a reliable performance. The latency is increased only to a small extent which demonstrated the ability of the model for scale effectively.
- **Comparison**: Traditional P2P models exhibit exponential latency increases with node growth.

Resilience to Sybil and 51% Attacks

- **Sybil Attack**: The model effectively mitigated Sybil attacks by restricting node creation per user based on unique user IDs.
- **51% Attack**: By limiting node control, the model ensured no single user could dominate the network.
- **Results**: Simulation results showed a significant reduction in the likelihood of successful Sybil attacks compared to models without node restrictions.

4.2 Critical Analysis

Improvement over Traditional Models

By incorporating the blockchain based decentralized authentication and efficient consensus mechanisms the Two-Stage model had enhances the security of the network. Vulnerabilities like identity spoofing and network manipulation are addressed as part of this research project. The mechanism which involved node restrictions majorly reduced the risk of Sybil and 51% attacks which also ensured the integrity of the network.

Privacy Preservation: At the validation phase the model uses the encrypted transactions by achieving the privacy without compromising the transparency. Where the data is publicly visible in the traditional systems this model showcased the balance among the privacy and integrity of the data and network.

Scalability and Efficiency: The latency low and high throughput was kept by the Two-Stage Model which is suitable for the real-world applications such as financial transactions, sharing the data related to the healthcare and secure communications. PoS consensus ensures that scalability efficiency by not involving the computational power consumption mechanisms like Proof of Work.

Comparison with Private Blockchains: Relying on the centralized control for the permissions of node and which limited to only trusted participants is done in the Private Blockchains. Whereas this two-stage model is operated within a decentralized environment which ensures the trust less authentication without involving the centralized authorities. Private blockchains also limit the access for security but in this Two-Stage Secure P2P model maintains the transparency of open participation while securing the network through decentralized authentication and node restrictions.

4.3 Summary of Findings

Metric	Two-Stage P2P Model	Traditional P2P Models
Latency	50 ms	100-200 ms
Throughput	500 TPS	250 TPS
Scalability	Stable with one hundred nodes	Performance degradation
Sybil Resilience	High (90% reduction in attacks)	Low (vulnerable to attacks)
51% Attack	Mitigated via node restrictions	Substantial risk if attackers dominate
Privacy	Encrypted transactions	Public transaction data

Table-2: Summary of Findings

4.4 Implications

Academic Perspective: A new technique/approach was provided by the Two-Stage Model to enhancing the security in block by also offering a proper solution to key vulnerabilities which are involved such as Sybil and 51% attacks.

Practitioner Perspective: In real-world applications as well, this model can be implemented which requires secure, scalable, and privacy-preserving data exchange.

5 Discussion

As per the results which are generated by the Two-Stage Secure Peer-to-Peer Model demonstrated the effectiveness by addressing the critical security and challenges which engage in scalability in the blockchain based decentralized networks. The following section will explore the implications of findings, potential applications, and the benefits of the proposed model. This also indicates the key areas very can be furtherly improved and real-world deployment considerations.

Security and Attack Resilience

The results which are presented as part of the simulation shows that the Two-Stage Model significantly enhances the security of the network. By implementing the decentralized peer-authentication and node restriction which can a user hold the model effectively mitigates:

- **Sybil Attacks**: Based on the unique and valid user IDs the node limitation mechanism would prevent a single actor from creating multiple fake nodes which reduced the risk of network manipulation. This differentiates from the traditional blockchain models where a sybil attack would compromise the process of consensus.
- **51% Attacks**: The mechanism of limiting only certain number of nodes a user can hold would ensure that no individual person can gain the majority by creating many nodes for a 51% attack. This safety measure will enhance the integrity and trustworthiness of network.

The dual-layered approach for authentication and transaction validation will strengthen the security of the network which also making it robust against identity spoofing and coordinated attacks.

Privacy and Data Integrity

This model maintains the balance among privacy and transparency through the transactions by encrypting them, so that during the validation process sensitive data will remain confidential while maintaining the data integrity by using the cryptographic verification. This makes the model suitable for the applications such as finance, healthcare, and secure communications.

Scalability and Performance

By using the consensus mechanisms which is efficient Proof of Stake (PoS) the model achieves:

- Reduced latency compared to computationally intensive Proof of Work (PoW).
- Consistent performance with up to one hundred nodes which demonstrates the scalability for real-time applications.

Comparison with Private Blockchains: Apart from the private blockchains, the Two-Stage Model maintains decentralization by enforcing limitation of nodes for security. It also combines the openness and transparency of public blockchains only with the controlled node management which also makes it flexible and thrustless.

Practical Implications

The model will have the practical applications in:

- **Decentralized Finance:** Enhancing transaction security and preventing fraud.
- **Healthcare: Enabling secure, confidential data sharing.**
- **Supply Chains:** Maintaining transparency while protecting against manipulation.

- **IoT Networks:** Ensuring secure communication between devices.

Limitations and Future Work

While the Two-Stage Model addresses many challenges, there are still areas for improvement:

- **Scalability under High Loads**: The future work can be explored in the optimization of the model even for the larger networks and transaction volumes which are higher.
- **Cryptographic Efficiency**: Further improvement in cryptographic techniques to reduce computational overheads during authentication and validation can be done.
- **Real-World Testing**: Deployment of the model in the natural environments which is close to the real-world environments will help in evaluating and establishing the efficiency in dynamic and unpredictable conditions.

The Two-Stage Secure P2P Model effectively offers a solution to enhance security, privacy, and scalability in decentralized networks. It solves some critical challenges like Sybil and 51% attacks which makes it suitable for security-critical applications.

6 Conclusion

The present research sought to answer the following question: "How can we guarantee security and privacy of data in blockchain technology, taking into account that it is distributed and immutable?" Address this the primary objective was to develop and evaluate a Two-Stage Secure Peer-to-Peer (P2P) Model using blockchain technology. The main aims were the realization of a decentralized peer authentication system, the avoidance of Sybil and 51% attacks, privacy-preserving transaction validation and network scalability with low latency.

Successfully designed and implemented the Two-Stage model which meets these objectives. In the initial stage, blockchain-based decentralized authentication was implemented using cryptographic techniques to ensure that each user could create only a limited number of nodes. This approach helps mitigate the risk of identity fraud and malicious activities. As part of the secondary stage the transactions are securely validated using the Proof of Stake by balancing the efficiency and security without requiring global consensus.

6.1 Key Findings

Following is effectively achieved by the model:

- **Enhanced Security**: By limiting node creation per user, the model mitigated Sybil attacks and reduced risk of 51% attacks which improved overall integrity of network.
- **Privacy Preservation**: Transactions are encrypted which ensured that the data is confidential in the process of transaction validation by maintaining the privacy and preserving the transparency.
- **Scalability**: By using the PoS consensus efficient mechanisms helped in achieving the low latency and consistent performance even in increasing the number of nodes.
- **Performance Evaluation**: The results that are obtained as part of the simulation in NS-3 demonstrated the ability of the model to support up to one hundred nodes by maintaining low transaction latency and by robust security measures.

Success in Achieving Objectives

The research has succeeded in its goals by realizing a model that balances decentralization, security, and scalability. The Two-Stage Model solves critical vulnerabilities blockchain-based P2P network applications, finding their usefulness in areas of high demanded security and privacy, e.g., finance, healthcare, and secure communication.

Future Work and Commercial Potential

While the current implementation shows promising results but there are several opportunities for future work:

- **Scalability Optimization**: Enhancing the model to manage larger networks and higher transaction volumes which can be evaluated in real-world.
- **Cryptographic Techniques**: By considering and implementing some more lightweight cryptography methods which can further reduce the computational overhead.
- **Real-World Deployment**: The model under the real-world conditions could be evaluated is recommended whereby considering the real-world public User-Id would be taken as the input and authenticated to create the nodes to evaluate its performance in dynamic environments.
- **Commercialization Potential**: The model can be used in the industries like Decentralized Finance, healthcare data management and IoT networks. Ability to in security enhancement and privacy in decentralized environments would make it a feasible solution to commercial applications requiring trust and integrity.

In conclusion, the proposed Two-Stage Secure P2P model would offer a robust, scalable and privacy preserving solution for the key challenges which are observed in blockchain based P2P networks. This research had provided a foundation for the further future advancements and potential commercial applications needed secure and decentralized data management.

References

AES Encryption: What is it & How Does it Safeguard your Data? (no date). Available at: https://nordlayer.com/blog/aes-encryption/ (Accessed: 10 December 2024).

Blockchain Security Issues - A Complete Guide (2021). Available at: https://www.getastra.com/blog/knowledge-base/blockchain-security-issues/ (Accessed: 10 December 2024).

Li, Junkai *et al.* (2023) 'A network-secure peer-to-peer trading framework for electricity-carbon integrated market among local prosumers', *Applied Energy*, 335(C). Available at: https://ideas.repec.org//a/eee/appene/v335y2023ics0306261922016774.html (Accessed: 10 December 2024).

nsnam (no date) *What is ns-3*, *ns-3*. Available at: https://www.nsnam.org/about/what-is-ns-3/ (Accessed: 10 December 2024).

Ping, J. *et al.* (2023) ‘A trusted peer-to-peer market of joint energy and reserve based on blockchain’, *Electric Power Systems Research*, 214, p. 108802. Available at: https://doi.org/10.1016/j.epsr.2022.108802.

Public, Private, and Permissioned Blockchains Compared (no date) *Investopedia*. Available at: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/ (Accessed: 10 December 2024).

Qushtom, H. *et al.* (2023) ‘A Two-Stage PBFT Architecture With Trust and Reward Incentive Mechanism’, *IEEE Internet of Things Journal*, 10(13), pp. 11440–11452. Available at: https://doi.org/10.1109/JIOT.2023.3243189.

Team, L.C.X. (2023) ‘Introduction to Private Blockchain’, *LCX*, 14 November. Available at: https://www.lcx.com/introduction-to-private-blockchain/ (Accessed: 10 December 2024).

The Bitcoin Blockchain: Where Do Transactions Get Recorded? - D-Central (2019). Available at: https://d-central.tech/where-are-bitcoin-transactions-recorded/ (Accessed: 10 December 2024).

Shokri, A., & Lati, S. (2021). Sybil attack detection in blockchain-based P2P energy trading. *IEEE Access*.

Unchaining Blockchain Security Part 3: Exploring the Threats Associated with Private Blockchain Adoption | Trend Micro (US) (no date). Available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/unchaining-blockchain-security-part-3-exploring-the-threats-associated-with-private-blockchain-adoption (Accessed: 10 December 2024).

Wang, Q. *et al.* (2024) ‘A Peer-to-Peer Trading Mechanism Considering Preferences: A Two-Stage Game Theory Approach’, in *2024 6th International Conference on Energy Systems and Electrical Power (ICESEP)*. *2024 6th International Conference on Energy Systems and Electrical Power (ICESEP)*, pp. 527–532. Available at: https://doi.org/10.1109/ICESEP62218.2024.10651950.

Wang, T. *et al.* (2021) ‘RBT: A distributed reputation system for blockchain-based peer-to-peer energy trading with fairness consideration’, *Applied Energy*, 295, p. 117056. Available at: https://doi.org/10.1016/j.apenergy.2021.117056.

‘What is ECDSA Encryption? How Does It Work?’ (2024), 4 March. Available at: https://www.encryptionconsulting.com/education-center/what-is-ecdsa/ (Accessed: 10 December 2024).

Xu, L. and Wang, B. (2023) ‘Peer-to-peer electricity trading considering voltage-constrained adjustment and loss allocation in blockchain-enabled distribution network’, *International Journal of Electrical Power and Energy Systems*, 152, p. 109204. Available at: https://doi.org/10.1016/j.ijepes.2023.109204.

Zhou, X. *et al.* (2024) ‘Bidirectional Privacy-Preserving Network- Constrained Peer-to-Peer Energy Trading Based on Secure Multiparty Computation and Blockchain’, *IEEE Transactions on Power Systems*, 39(1), pp. 602–613. Available at: https://doi.org/10.1109/TPWRS.2023.3263242.

Appendix

```
sqlite> select * from Users;
DefaultUser1|0|-----BEGIN PUBLIC KEY-----
MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEgryQorHBhbefw2aRwTe6oIojB1qQLCbe
GyNeRMbG5aXXEgTeE1GaHA05E5l2Jn8d4ij9kCvQUu6esJ2pBkG/bw==
-----END PUBLIC KEY-----

DefaultUser2|0|-----BEGIN PUBLIC KEY-----
MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEqMh7e74KUiNpE2br1oUqp15xfchMDkKV
aRIaaiKYUMPGAeDY8SUMtannTW5Wzj+eZQLw0PM4JR3y8D4D+ebGAw==
-----END PUBLIC KEY-----

Amma|3|-----BEGIN PUBLIC KEY-----
MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAERej4kAAfv75iw+U2+yZL/pY9fC61zXjb
+Q5xen2dEiaxofjML0d1dN9cTjQCZYiT3Hq9F0TBvsn0BcPnBz8JdA==
-----END PUBLIC KEY-----

Durga|4|-----BEGIN PUBLIC KEY-----
MFYwEAYHKoZIzj0CAQYFK4EEAAoDQgAEuv7xagnMDrg7J2dPqDJeFr69azFln4oF
EYRh0UPwe5HFkrLhPUbYKeNfcxfTMwMybaBfh8dYRxhqp2+JKs2chA==
-----END PUBLIC KEY-----
```

Figure-7: Sample database with usernames, node count and Public Key

```
sqlite> select * from Transactions;
1|Amma|DefaultUser2|e◆◆M
w◆&y◆@◆                 ◆◆◆◆◆
◆◆◆◆2Đ◆g◆|MEUCIQCZJd6/v+OhslbNsAQXtqMisdwTkCuJqxupQmnywJL2ZgIgdqIOG5y+fAKf
AitS4fUOkp7fL2Fzz3qrmqof1+qAMPI=

2|Amma|DefaultUser1|e◆◆M
w◆&y◆@◆                 ◆◆◆◆◆
◆◆◆◆2Đ◆g◆|MEYCIQCNm4tc+1joUbyuilZ0SPG/PVzlujZXZhqK+U/DoZTrygIhAOb7+N1qGUfl
JbCnPpSi5AEffDixLKp8Bs1rG/gW4zE5

3|Durga|Amma|e◆◆M
w◆&y◆@◆          ◆◆◆◆◆
◆◆◆◆2Đ◆g◆|MEYCIQDYAgek24nyalCGu5SR7iTG/zZ6zHd2fyjoz03IjHllrgIhAKDPiLOMB/Pq
zMnC6j14NRRZdbZhbvOWoiRK54X97/o4

4|Durga|DefaultUser1|e◆◆M
w◆&y◆@◆                 ◆◆◆◆◆
◆◆◆◆2Đ◆g◆|MEUCIGaEa8rp/Erl3nhViRrL+VG+LUJ2Ch7DX8Z42jOFau1gAiEA6+icDfZApefP
ulsyHmGJSZH1+w1A/jOT9kU6lCAPgVc=

5|Durga|DefaultUser2|e◆◆M
```

Figure-8: Transactions table where all the transactions are encrypted and stored

```
sqlite> select * from Merkleroots;
1|3d54f45d2beb7cdf9dad5f96cdbaa5da0791b76397c68a9855696005b31e967b|2024-12-09 15:45:04
2|3d54f45d2beb7cdf9dad5f96cdbaa5da0791b76397c68a9855696005b31e967b|2024-12-09 15:45:04
3|3d54f45d2beb7cdf9dad5f96cdbaa5da0791b76397c68a9855696005b31e967b|2024-12-09 15:45:04
4|3d54f45d2beb7cdf9dad5f96cdbaa5da0791b76397c68a9855696005b31e967b|2024-12-09 15:45:04
5|3d54f45d2beb7cdf9dad5f96cdbaa5da0791b76397c68a9855696005b31e967b|2024-12-09 15:45:04
6|2b930ebb2729e31ea7659da56144d60bcf3bac4db896c828522f1887c6447dcc|2024-12-09 15:45:04
7|79a57d08b835b2198c75dec924784a2aebeb91999903ebff4caf1af70c11d9df|2024-12-09 15:45:04
8|59f42e1f8c91c0c789b05ccd063d3ad383d24b209098be34575d905bf1b33fc9|2024-12-09 15:45:04
9|59f42e1f8c91c0c789b05ccd063d3ad383d24b209098be34575d905bf1b33fc9|2024-12-09 15:45:04
10|5aff11a13e47e99d95401c173f5804979387451e07a0936efa6a5bb85819a465|2024-12-09 15:45:05
11|5aff11a13e47e99d95401c173f5804979387451e07a0936efa6a5bb85819a465|2024-12-09 15:45:05
12|0cd89355848db5fa378185e5484a4182583da72fef20ce19e01ea4adbd9b8d72|2024-12-09 15:45:06
13|4c6ef57a76d365791d3fc090f5e473e875671a12d08cd0e60f7cfa561c9604c1|2024-12-09 15:45:07
14|fb975b3a26d94d39cdc1ab5658f603b351b28ca00122abad9b9c8a8bd4549c16|2024-12-09 15:45:08
15|184e3353e6dc5c4461f208c4551a975134ac756ee8962de45799106d69837e68|2024-12-09 15:45:10
16|184e3353e6dc5c4461f208c4551a975134ac756ee8962de45799106d69837e68|2024-12-09 15:45:10
17|184e3353e6dc5c4461f208c4551a975134ac756ee8962de45799106d69837e68|2024-12-09 15:45:10
18|ecd17d88fd83368ed195cd58c7a424e9a927a5533891e380997e19518a2b01cc|2024-12-09 15:45:14
19|c4ba11ca35c63568131bb86f0c982886fb0e939a4116dbce3f332076f30b2c5a|2024-12-09 15:45:16
20|c4ba11ca35c63568131bb86f0c982886fb0e939a4116dbce3f332076f30b2c5a|2024-12-09 15:45:16
21|c4ba11ca35c63568131bb86f0c982886fb0e939a4116dbce3f332076f30b2c5a|2024-12-09 15:45:16
22|a888684b4ac40c7e69fef448aca001fc28cac31a1dcc5f2f0ca9387987e014c9|2024-12-09 15:45:25
23|7fe31956ca029b9fd525c0866c5d40806859608478869e459058f369d50fdfa5|2024-12-09 15:45:29
24|7fe31956ca029b9fd525c0866c5d40806859608478869e459058f369d50fdfa5|2024-12-09 15:45:29
25|6e0551be9a94d85248b1fe8b4377a621ea4724e4537e172b475c2e230d4a92a7|2024-12-09 15:45:32
```

Figure-9: Merkle roots which are calculated and stored