Islamic University of Technology (IUT)

Department of Computer Science and Engineering (CSE)

PBFT and Homomorphic Encryption with Private Blockchain in the Context of E-Voting Systems

Authors

Shihab Ahmed - 190041225

Lutful Awal Rafi - 190041210

Alin Mohammed Sifayet - 190041222

Supervisor

Dr. Muhammad Mahbub Alam

Professor, Department of CSE

Islamic University of Technology

Co-Supervisor

S. M. Sabit Bananee

Lecturer, Department of CSE

Islamic University of Technology

Declaration of Authorship

This is to certify that the research done by **Shihab Ahmed, Lutful Awal Rafi**, and **Alin Mohammed Sifayet** under the supervision of **S.M. Sabit Bananee**, Lecturer, Department of Computer Science and Engineering (CSE), Islamic University of Technology (IUT) and **Dr. Muhammad Mahbub Alam**, Professor, Department of Computer Science and Engineering (CSE), Islamic University of Technology (IUT),resulted in the work presented in this thesis. It is further declared that no part of this thesis or the entire thesis has ever been submitted to another institution for a degree or diploma. A list of references is provided, and information taken from both published and unpublished works of others is recognized in the text.

Authors:

Shihab Ahmed
Student ID- 190041225

Lutful Awal Rafi
Student ID- 190041210

Alin Mohammed Sifayet
Student ID- 190041222

Supervisor:

Dr. Muhammad Mahbub Alam
Professor
Department of Computer Science and Engineering
Islamic University of Technology (IUT)

Co-supervisor:

S. M. Sabit Bananee
Lecturer
Department of Computer Science and Engineering
Islamic University of Technology (IUT)

Acknowledgement

We express our deepest gratitude to **Professor Dr. Muhammad Mahbub Alam** for his exceptional guidance, mentorship, and invaluable contributions throughout our thesis work. As a professor in the department of computer science and engineering at IUT, his extensive knowledge and expertise have been instrumental in shaping our research and academic journey.

From the very beginning stages of our thesis, Dr. Muhammad Mahbub Alam provided us with inspiration and direction. His profound understanding of the subject matter and his ability to offer valuable insights helped us refine our thesis theme and select a suitable subject. His guidance extended to proposing algorithms, making necessary modifications, and providing continuous support throughout the project's implementation and finalization.

We are truly grateful for Professor Dr. Muhammad Mahbub Alam's unwavering commitment to our success. His unwavering dedication to our academic pursuits, his willingness to invest his time and effort in reviewing our work, and his constant availability for discussions and clarifications have been immensely helpful.

Furthermore, we extend our thanks to **SM. Sabit Bananee**, Lecturer in the Department of Computer Science and Engineering at IUT. His insightful review of our proposal and simulation techniques played a vital role in shaping our research approach. His encouragement and support motivated us to persevere and continue our hard work.

The authors acknowledge the significant contributions of Dr. Muhammad Mahbub Alam and S.M. Sabit Bananee to our thesis work. Your guidance, advice and input have been invaluable in ensuring the successful completion of our research. We are truly grateful for their mentorship and are honored to have had the opportunity to learn from them.

Contents

List of Figures

Abstract

In the digital age, preserving faith in democratic systems w on the fairness and openness of election procedures. This research presents the design of a blockchain based electronic voting system that leverages the Practical Byzantine Fault Tolerance consensus mechanism and homomorphic encryption to ensure transparent and tamper proof elections. Our system addresses critical security challenges, including integrity, non-repudiation, confidentiality, authenticity, and authorization, making it particularly suited for environments where trust is essential. [7]

The core of our approach lies in combining PBFT, which offers fault tolerance and efficient consensus, with homomorphic encryption, which enables the secure handling of votes without compromising voter privacy. Experiments were conducted to evaluate the system's performance, focusing on transaction throughput and block generation time. The results indicate that our system significantly outperforms traditional consensus mechanisms such as Proof of Work in both efficiency and scalability.

Furthermore, this thesis outlines future work to address emerging challenges and enhance the system's capabilities. [8] These include the implementation of quantum-resistant cryptography, sharding for improved scalability, using machine learning methods for enhanced security, and ensuring cross-browser compatibility for broad accessibility.

Overall, this research demonstrates that a blockchain-based e-voting system, fortified by PBFT and homomorphic encryption, can provide a secure and reliable platform for conducting elections in the digital era. By advancing the development of such systems, we aim to contribute to the future of transparent electoral processes.

Chapter 1

Introduction

1.1 Introduction to Electronic Voting Systems

Electronic voting systems are platforms that allow voters to cast their votesw electronically, either through dedicated voting machines or via the internet. [9] The adoption of e-voting systems has been driven by the need to heighten the efficiency, accessibility, and security of the voting process. Traditional paper based voting methods are often slow and prone to errors, leading to delays in results and potential disputes. In contrast, e-voting systems smoothen the process, enabling faster ballot counting, reducing human error, and potentially increasing voter turnout by making voting more accessible.

1.2 Historical Evolution of E-Voting Technologies

The evolution of electronic voting systems began with the introduction of mechanical voting machines in the early 20th century, followed by the development of Direct Recording Electronic (DRE) systems in the 1970s. [10] These systems allowed voters to make their selections via a touchscreen or other input devices, with votes being recorded directly into the machine's memory. Optical scan systems, introduced later, combined the reliability of a paper trail with the efficiency of electronic counting, further enhancing the voting process. In recent years, internet-

based voting systems have emerged, allowing voters to cast their ballots remotely using a computer or mobile device. While these systems offer unprecedented convenience, they also present significant security challenges, such as the risk of cyberattacks, data breaches, and manipulation of results. These concerns have limited the widespread adoption of internet voting, particularly in large-scale national elections.

1.3 Blockchain Technology for Secure and Transparent E-Voting

Blockchain technology is a digital ledger. It records transactions across numerous computers in a manner that precludes retroactive tampering [9].It was first developed as the basis for digital currencies such as Bitcoin. Blockchain technology has the potential to improve election security and transparency in the context of electronic voting. [11] By using blockchain, votes can be recorded in an immutable ledger. Blockchain's transparency allows independent observers to verify the accuracy of the vote count, increasing trust in the election process. Blockchain can also address concerns related to voter privacy and vote integrity. [12] Through the use of advanced cryptographic techniques, blockchain can ensure that voter identities remain confidential while simultaneously protecting the integrity of the votes. Consensus mechanisms can be used to validate votes across the network, ensuring that only legitimate votes are counted. Most blockchain-based electronic voting systems use simple consensus techniques PoA and PoW, however they either promote centralization or consume excessive amounts of energy [10].

1.4 Homomorphic Encryption and Blockchain

Blockchain Technology and homomorphic encryption has been used in together to solve e-voting problems. But [13] has implemented a system where the non-repudiation of the vote is compromised as the vote itself is not encrypted despite

the fact that the voter's identity has been encrypted accordingly. The use of homomorphic encryption to simplify the counting of votes is also a good idea. As homomorphic encryption allows mathematical manipulation, adding the encrypted votes will keep them countable. But confidentiality will be compromised if the voter's information is not safeguarded. This is the approach that can be encountered in [14]. A similar but slightly different approach can be seen in [15]. The homomorphic characteristic is utilized here to count the votes without decrypting each individual vote and the blockchain is also used as a second level of security measure here for preserving votes. In the context of Bangladesh, achieving both the privacy of the voter, the non-repudiation and integrity of the vote are also essential which requires a different approach. The scope of homomorphic encryption and blockchain combined is still at large in the e-voting system in the context of Bangladesh.

1.5 Research Objectives, Scope, and Significance

The specific objectives of the research are:

1. To Analyze Existing E-Voting Systems: Examine the strengths and weaknesses of current e-voting systems, with a particular focus on security, transparency, and voter trust.

2. To Investigate Blockchain's Use in E-Voting: Look into how blockchain technology might help address the shortcomings of the current electronic voting systems, particularly in terms of enhancing security, safeguarding voter privacy, and enhancing election process transparency.

3. To Implement a PBFT-Based E-Voting System: Develop a prototype e-voting system that uses the PBFT consensus mechanism to achieve fault tolerance and secure vote validation in a decentralized environment.

   Determine any areas where the suggested system could be improved, and make recommendations for future lines of inquiry and advancement in the

field of blockchain-based electronic voting.

While the principles of the study are broadly applicable, the research is particularly tailored to the context of Bangladesh. The study considers the specific challenges and requirements of implementing an e-voting system in a developing country, including infrastructure limitations, voter education, and political considerations. The study includes the design and implementation of a prototype e-voting system. This prototype is used to validate the concepts and techniques proposed in the research. The study entails assessing the suggested electronic voting system's effectiveness, scalability, and security. Large-scale deployment and practical system testing are not included in the scope, nevertheless. The study helps the ongoing development e-voting systems by applying blockchain technology.This study has the potential to improve election integrity and credibility by addressing the shortcomings of the present electronic voting technologies. The study demonstrates how blockchain technology can be applied to critical areas beyond finance, such as e-voting. This expands the understanding of blockchain's potential and encourages further exploration of its applications in various fields. In the context of Bangladesh, where the integrity of the electoral process is often questioned, this research provides a framework for implementing a secure and transparent e-voting system. The findings could have significant implications for improving the credibility of elections in Bangladesh and other developing countries facing similar challenges. The research takes forward future studies in the field of blockchain-based e-voting. By identifying areas for improvement and suggesting directions for further research, this study encourages continued innovation in the development of secure and reliable voting systems.

Chapter 2

Preliminaries

2.1 Blockchain Technology [1]

2.1.1 Definition of Blockchain Technology

Blockchain technology is a digital ledger that records transactions on multiple computers in a way that ensures the security. Blockchain functions in a p-p network, where each member (node) has access to the complete ledger, in contrast to conventional systems where a single entity controls the data. [16] Participants can trust the system without having to trust one another individually thanks to this decentralized method, which also eliminates the need for intermediaries. A group of transactions is present in each of the blocks that make up a blockchain. A chain is created by connecting these units in chronological sequence. A block contains a hash of the one before it, which guarantees that once the information is stored, it cannot be changed without affecting all following blocks, which would require network consensus. [17] [18]

2.1.2 Components of Blockchain Technology

Blocks: The fundamental unit of a blockchain. A block contains a collection of transactions. It also has a timestamp and a reference to the previous block. All of them are important. The start block is known as the genesis block.

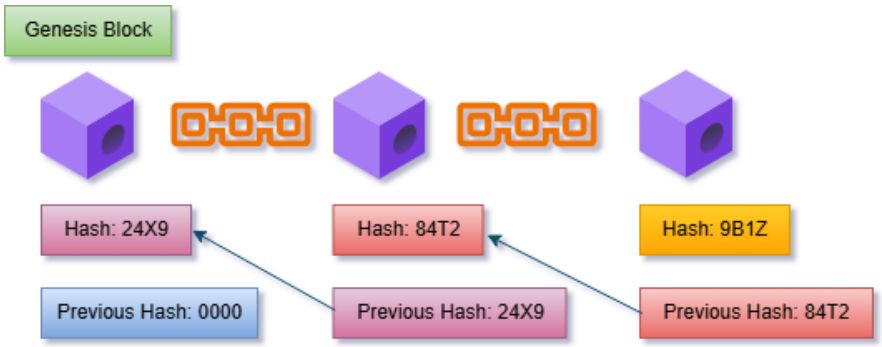

Figure 2.1: Components of a Blockchain

Transactions

Transactions are the actions recorded on the blockchain. In the context of cryptocurrencies, these are transfers of digital assets from one party to another. In other applications, transactions could represent any data exchange, such as a vote cast in an election.

Nodes

Nodes are the computers or devices that participate in the blockchain network. Each node maintains a copy of the entire blockchain and can validate and propagate transactions.

Consensus Mechanism

The method by which the network's nodes concur on the legitimacy of transactions and the sequence in which they should be appended to the blockchain. Different blockchains use different consensus mechanisms.

Cryptographic Hash Function

An algorithm that transforms data into a string of characters. Each block holds the hash of the previous block. This creates a secure link between them. If any part of a block is altered, its hash will change, breaking the chain. [19]

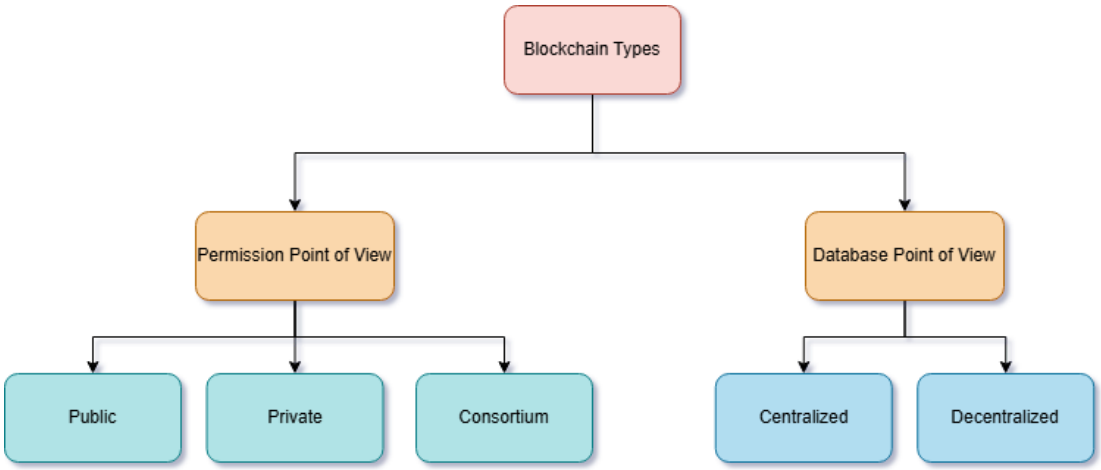

Figure 2.2: Types of Blockchain

Smart Contracts

Just like real-life contracts, they impose predefined rules and regulations. They exist digitally and are initiated or voided automatically when the suitable conditions are met.

2.1.3 Types of Blockchains [2]

Public Blockchains

These are open to anyone and fully decentralized, allowing anyone to join, participate, and view the transactions on the network.

Private Blockchains

These are restricted networks where only allowed participants can join. They can then validate transactions. Private blockchains are often used by organizations that require greater control over the network, such as in supply chain management or enterprise applications. They offer faster transaction processing but are less transparent than public blockchains.

Consortium Blockchains

A hybrid between public and private blockchains. They are controlled by a group of organizations. A single entity cannot control it. Access to the network is restricted to the consortium members. Consortium blockchains are commonly used in industries where multiple organizations need to collaborate, such as in banking or trade finance. [20]

Hybrid Blockchains

Hybrid blockchains take the good from both of the aforementioned. They allow for a mix of private permissioned access and public transparent transactions. This type of blockchain is suitable for use cases where certain data needs to be publicly accessible while other data remains confidential. [21]

2.2 Consensus Mechanisms

2.2.1 Proof of Work (PoW)

One of the oldest and most popular consensus methods is Proof of Work (PoW), which is well known for being employed in Bitcoin [22]. The first person to solve a challenging cryptographic challenge wins the privilege to add the next block to the blockchain in a proof-of-work (PoW) competition amongst nodes, or miners. This procedure uses a lot of energy because it needs a lot of processing power. [23]

1. Those who are miners solve complex puzzles to add a new block to the chain.
2. Requires a lot of power and energy.
3. The first one to solve the problem and may also validate the block is often rewarded with cryptocurrency (e.g., Bitcoin).
4. Ensures network security but can lead to inefficiency (high energy usage).

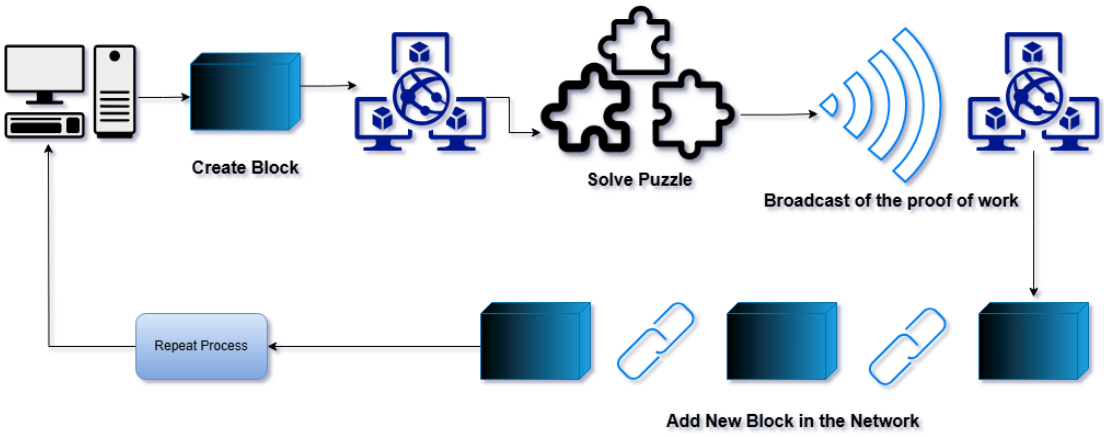

Figure 2.3: Workflow of Proof of Work

Pros

1. High level of security and resistance to attacks.
2. Proven track record in large-scale public blockchains.

Cons

1. Energy-intensive and environmentally unsustainable.
2. Slow transaction processing, leading to scalability issues.

2.2.2 Proof of Stake (PoS) [3]

A consensus method called Proof of Stake chooses validators taking into account the amount of currency they are willing to stake. Based on their stake, validators are selected to produce new blocks and validate transactions [24]; frequently, a degree of randomization is incorporated into the selection process. [25]

1. Validators are picked so that they can produce new blocks taking into account the volume of cryptocurrency they stake (lock up as collateral).
2. No mining is involved; instead, it's based on ownership and randomness.
3. The more you stake, the higher your chance of being selected as a validator.

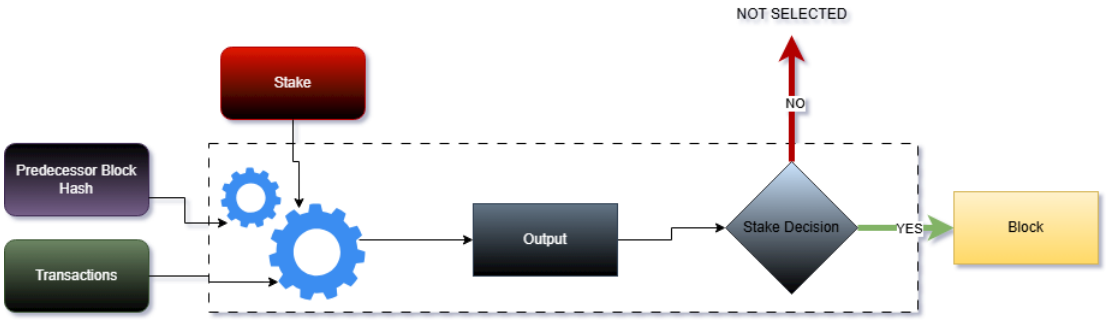

Figure 2.4: Workflow of Proof of Stake

4. It uses less energy than POW because it works differently without requiring any extreme computational work.

Pros

1. More energy-efficient compared to PoW.
2. Faster transaction processing.

Cons

1. Can result in centralization when power is concentrated among those with higher resources.
2. The "nothing at stake" issue, in which contradicting chains may be validated by validators. [26]

2.2.3 Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance is another one of the consensus mechanism designed to function efficiently in environments where nodes may fail or act maliciously. Through a series of procedures known as pre-prepare, prepare, and commit (PBFT), a number of nodes (validators) must concur on the authenticity of a transaction before it is put to the blockchain. Up to one-third of all nodes may be malevolent or defective, yet the system can withstand this without jeopardizing the integrity of the consensus process. [27]

1. Designed to withstand up to 1/3 of nodes being faulty or malicious.
2. Consensus is achieved through a series of rounds where different types of messages are exchanged to get to the new block.
3. Each node has a state and can propose, vote, and validate new blocks.
4. Suitable for permissioned blockchains and private networks, providing fast and reliable finality.

2.2.4 Why PBFT is Suitable for E-Voting:

1. Fault Tolerance: PBFT's ability to handle malicious or faulty nodes is crucial in an electronic voting scheme, where ensuring the accuracy and integrity of votes is paramount.
2. Efficiency: Unlike PoW, PBFT does not require computationally intensive tasks, making it more efficient and scalable for handling a large number of votes in a short period.
3. Security: PBFT makes sure of the nodes agreeing on the order and validity of transactions, reducing the risk of tampering with votes and ensuring that the election results are trustworthy.
4. Low Latency: PBFT can achieve consensus quickly, which is important for timely election results.

2.3 Encryption

2.3.1 Introduction to Encryption

Encryption is a fundamental technology used to ensure the security and confidentiality of data in various systems, including electronic voting (e-voting). It involves converting plaintext data into an unreadable format (ciphertext) using an algorithm and a cryptographic key. Only those with the corresponding decryption

key can convert the data back into its original form. In the context of e-voting, encryption plays a critical role in protecting voter privacy, ensuring the integrity of the votes, and preventing unauthorized access or tampering.

2.3.2 Role of Encryption in E-Voting

By implementing encryption, e-voting systems can guarantee secure communication, protect voter identities, and ensure the integrity of election results, making encryption an essential component for the trustworthiness of the entire voting process.

2.4 Homomorphic Encryption

2.4.1 Introduction to Homomorphic Encryption

Homomorphic encryption is a type of encryption which allows manipulations on encrypted data but we wont need to decrypt it beforehand. We can perform operations like addition or multiplication on the ciphertext, and when the result is decrypted, it matches the outcome of the same operations performed on the plaintext. In traditional encryption schemes, data must be decrypted before any computation can be performed, which exposes it to potential security risks. Homomorphic encryption, on the other hand, allows for secure computation on encrypted data, making it particularly valuable in scenarios where data privacy is a critical concern.

Preservation of Voter Privacy

In an e-voting system, it is crucial to ensure that votes remain confidential and that voter identities cannot be traced back to their votes. Homomorphic encryption allows the voting process to be carried out in a way that preserves voter privacy, as the votes can be tallied without ever decrypting individual votes.

Secure Vote Counting

One of the main challenges in e-voting is ensuring that votes are counted accurately without compromising the secrecy of each vote. Homomorphic encryption enables the secure aggregation and tallying of votes. The final tally can be decrypted to reveal the election results without revealing individual votes, maintaining the confidentiality and integrity of the election process.

Resistance to Tampering

Homomorphic encryption approves computations on encrypted data. As a result, it prevents tampering during the counting process. It doesn't matter if an attacker gains access to the encrypted votes because they cannot alter the outcome without knowing the decryption keys, which remain secure.

Future-Proofing Against Quantum Computing

As quantum computing advances, traditional encryption methods may become vulnerable. Homomorphic encryption is considered a future-proof technique that could safeguard e-voting systems against quantum threats
In conclusion, homomorphic encryption is a powerful tool for ensuring the privacy and security of e-voting systems. By enabling secure computations on encrypted data, it helps maintain the confidentiality of votes while ensuring accurate and tamper-proof election results. Combined with the PBFT consensus mechanism in a blockchain-based e-voting system, homomorphic encryption can provide a robust and secure solution for modern electoral processes. [28]

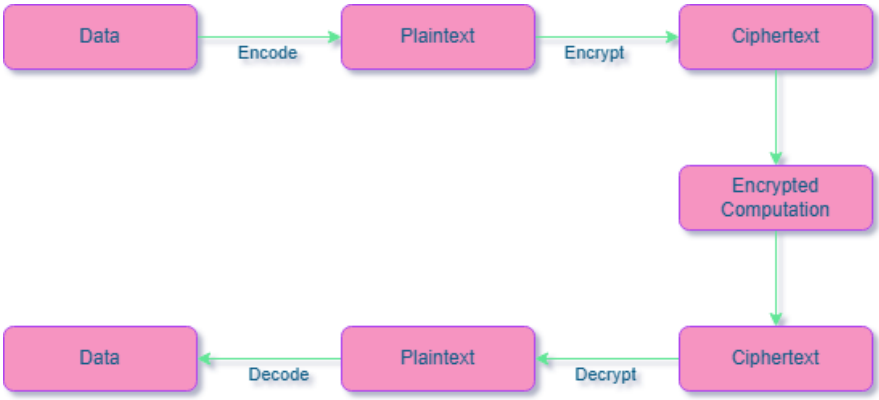

Figure 2.5: Workflow of Homomorphic Encryption

Chapter 3

Related Works

3.0.1 Review of Existing E-Voting Systems

E-voting systems have evolved over time, with numerous models being proposed and implemented to enhance the efficiency, security, and accessibility of the voting process. However, these systems vary significantly in their design, functionality, and security features. [29] [18]

Direct Recording Electronic (DRE) Systems

1. Overview: DRE systems are electronic voting machines that record votes directly into the system's memory. Voters interact with the machine via a touchscreen or other input devices, and their selections are stored electronically.

2. Security Features: DRE systems often incorporate basic encryption techniques to protect the integrity of votes and prevent tampering.

3. Limitations: DRE systems have been criticized for their vulnerability to hacking, as the electronic records can potentially be altered without leaving any trace. Additionally, the reliance on proprietary software means that the voting process is not fully transparent, leading to concerns about the trustworthiness of the system. The absence of a decentralized mechanism also makes these systems susceptible to single points of failure.

Optical Scan Voting Systems

1. Overview: Optical scan systems use paper ballots that voters mark manually. These ballots are then scanned by electronic machines that count the votes. The physical ballots provide a reliable backup in case of disputes.

2. Security Features: The primary security feature of optical scan systems is the paper ballot, which allows for manual recounts and audits. The use of encryption in the scanning and counting process further secures the electronic records.

3. Limitations: While optical scan systems provide a tangible audit trail, they still rely on centralized servers for counting and storing votes. This centralization presents a risk of tampering, either during the scanning process or within the central servers. Additionally, these systems can be expensive to implement on a large scale.

Internet-Based Voting Systems:

1. Overview: Internet voting systems allow voters to cast their votes remotely. These systems are designed to increase voter accessibility, particularly for those who cannot physically attend polling stations.

2. Security Features: Internet voting systems typically use encryption to secure data transmission between the voter's device and the server. Multi-factor authentication (MFA) is often employed to ensure that only authorized voters can cast a ballot.

3. Limitations: Internet voting faces significant problems related to security. The potential for cyberattacks, such as Distributed Denial of Service (DDoS) attacks, MOM attacks, and malware, poses a major risk. Additionally, ensuring voter anonymity while maintaining the integrity of the vote is a complex issue. The lack of a decentralized structure also makes these systems vulnerable to centralized points of failure and manipulation.

3.1 Blockchain in E-Voting

3.1.1 Design of Secure Electronic Voting System Using Multifactor Authentication and Cryptographic Hash Functions [4]:

Methodology

This study proposed an e-voting system that incorporates multifactor authentication (MFA) to verify voter identity and cryptographic hash functions to secure vote transmission. The system ensures that each vote is encrypted end-to-end, maintaining voter privacy.

Overview of the Electronic Voting System

With careful design, the electronic voting system makes voting safe via wired and wireless networks accessible to voters and administrators alike. Ensuring a secure system with seamless cross-platform functionality is the main goal of this design. This tiered strategy aids in methodically overseeing the many phases of the voting procedure, guaranteeing security and integrity at every turn.

Pre-Election Phase

Voter registration and authentication are important aspects of the pre-election phase. In this stage, the system offers a venue for prospective voters to register their names. In order to verify that they are eligible to vote, voters must enter necessary information such as their phone numbers and email addresses. Each voter receives a unique ID from the system automatically after their registration data are submitted. A distinct grid card code is also generated, matching the unique ID exactly. The technology generates a one-time PIN—a random string of ASCII characters—and sends it to the voter via SMS in order to increase security even further. This PIN acts as the voter's authentication credential along with the grid card code and unique ID. All these details are securely stored in the database,

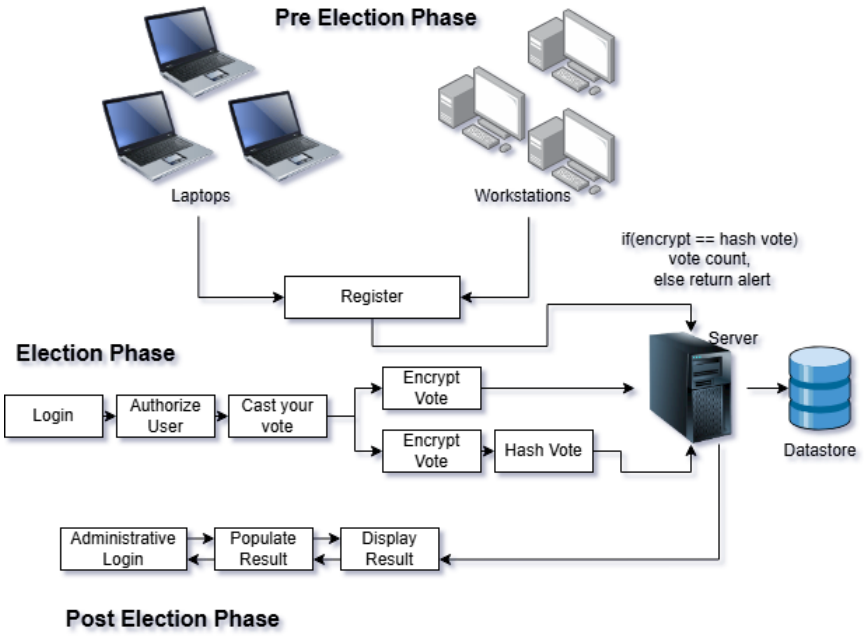

Figure 3.1: Architecture of the secure voting system

ensuring that only eligible and authenticated voters can proceed to the voting phase.

Election Phase

The real voting procedure comes into focus during the election period. Voters use the grid card code, SMS PIN, and unique ID to authenticate themselves. Only approved voters are able to cast ballots thanks to this multi-factor authentication, which guarantees the security of the voting process. Voters use the electronic ballot to make their selections after being authenticated. Votes are encrypted using a private key as soon as they are cast in order to protect their integrity and confidentiality. For extra protection, the encoded vote is then split into two halves. The SHA256 technique is used to hash a portion of the encoded output, yielding a 256-bit random number. The vote is kept safe and impenetrable thanks to the combination of hashing and encryption.

Post-Election Phase

Voter integrity is preserved by means of vote verification and processing, which take place during the post-election period. In order to make sure that the votes haven't been tampered with during transit, the system compares the encoded votes that were received with their matching hashes at the start of this phase. The SHA256 technique is used to hash the encrypted votes after they have been decoded. The hash that was sent during the election phase is compared to the one that was generated. When the hashes line up, the vote is verified and tallied. The vote is marked as maybe tampered with and is not counted if there is a difference and the hashes do not match. This meticulous verification procedure guarantees that only legitimate votes are taken into account in the final tally. The system also maintains a comprehensive audit trail, logging all operations from voter registration to vote counting.

Strengths

A layer of protection is added by using MFA and cryptographic hash functions, which make it more difficult for unauthorized people to vote or alter data that has been delivered.

Weaknesses

The system does not fully ensure non-repudiation, meaning that voters could potentially deny having cast their votes. Additionally, the reliance on traditional encryption methods rather than a decentralized ledger makes the system vulnerable to central points of failure.

3.1.2 Go-Ethereum for Electronic Voting System Using Clique as Proof-of-Authority [5]

Methodology

This study utilized the Go-Ethereum platform with a proof-of-authority (PoA) consensus mechanism to create a blockchain-based e-voting system. The PoA mechanism allows only a fixed number of validators to propose blocks, thereby ensuring efficiency and low energy consumption.

Ethereum Blockchain

The traditional use of blockchain technology has primarily been confined to the realm of cryptocurrencies, where it has demonstrated its prowess in enabling secure and decentralized transactions. [30] However, this study represents a departure from this conventional application by proposing an electronic voting system that harnesses the power of Ethereum blockchain on a decentralized server. Ethereum, conceptualized by Vitalik Buterin in 2014, stands out as a public peer-to-peer network characterized by its native digital currency, Ether. Unlike its predecessors, Ethereum was intended to be a flexible platform that could execute smart contracts—basically, self-executing agreements with predetermined conditions—rather than just a means of trade. This special characteristic makes it possible to create decentralized applications in a number of fields, including as supply chain management, banking, and now voting systems.

Efficiency is another compelling advantage offered by blockchain-based voting systems, as they streamline and optimize the electoral process, minimizing operational costs and logistical challenges associated with traditional voting methods. By encoding the rules and conditions of the voting process into self-executing contracts, smart contracts ensure that the electoral process is conducted fairly and efficiently.

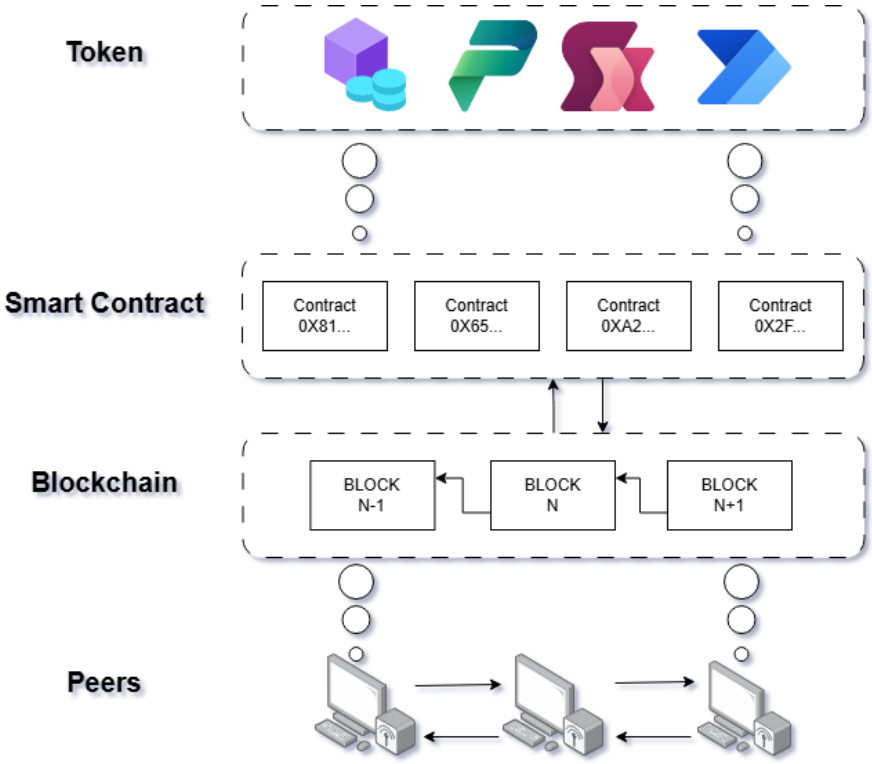

Figure 3.2: Ethereum Blockchain Workflow

Proof of Authority and Clique

Apart from the innate advantages of blockchain technology, the Proof-of-Authority (PoA) consensus algorithm's use makes blockchain-based voting systems even more secure and scalable. PoA, a reputation-and credibility-based consensus method, makes sure that only verified and vetted individuals are allowed to confirm transactions and uphold the blockchain's integrity. PoA gives greater weight to reputation and experience. This reduces the possibility of bad actors or Sybil attacks. [31] This consensus approach reduces the computing complexity associated with conventional consensus procedures, hence facilitating scalability while simultaneously guaranteeing the voting process's dependability and security. [29]

A predetermined group of reliable nodes known as authorities serves as the foundation for the Proof-of-Authority (PoA) algorithm's operation. Every authority in the network is given a distinct identification that helps to identify them. The system's integrity depends on the presumption that most of these authorities are morally upright individuals. In particular, consensus is reached when a transac-

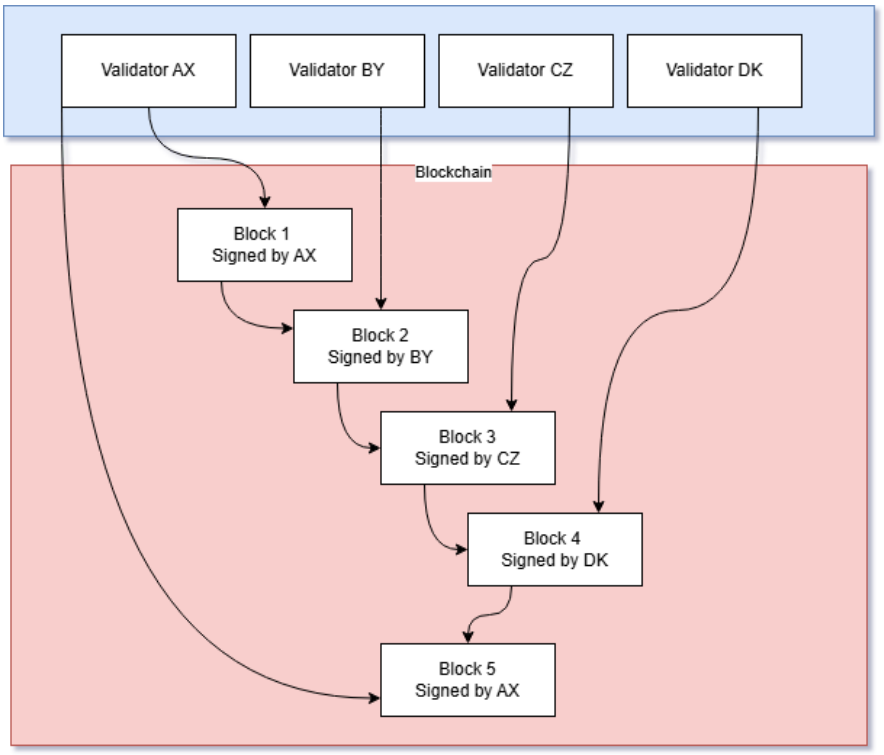

Figure 3.3: Proof of Authority Using Clique

tion is approved by at least (N/2)+1 authorities, where N is the total number of authorities in the network. The PoA method uses a rotation mining scheme, in which time is divided into discrete periods, with an elected authority acting as the mining leader during each interval, to promote consensus. An implementation of the PoA algorithm variation Clique is found in Geth, a GoLang-written Ethereum blockchain client. The Clique algorithm divides up the effort of suggesting and approving blocks among the network's validators.

Overview of Proof of Authority (PoA)

- **Consensus Mechanism:**
  - To validate transactions and generate new blocks, the PoA consensus method depends on a small group of pre-approved validators, or authorities.
- **Trusted Validators:**

  - Validators are known entities, often public or well-known organizations. They are somewhat trustworthy.
  - Because the identities of validators are public, there is a strong incentive for them to act honestly, as their reputation is at stake.

- **Efficiency:**
  - PoA is highly efficient compared to PoW because it doesn't require solving complex mathematical puzzles, leading to faster block times and lower energy consumption.
  - The consensus process is streamlined since only a few validators participate in creating blocks.

- **Scalability:**
  - Due to its efficiency, PoA is well equipped for private and also consortium blockchains where scalability and fast transaction throughput are important.
  - It is often used in enterprise settings or situations where a group of trusted entities govern the network.

- **Security Considerations:**
  - While PoA is secure in trusted environments, it is less decentralized than other consensus mechanisms, making it potentially vulnerable to collusion among validators.
  - The system relies heavily on the honesty and integrity of the validators, which could be a concern in less controlled environments.

Overview of Clique

- **Ethereum Implementation:**
  - Clique is Ethereum's implementation of the PoA consensus algorithm, designed for use in private networks or consortium blockchains.

  - It is integrated within the Ethereum protocol, enabling developers to create PoA-based Ethereum networks.

- **Block Creation:**
  - In Clique, blocks are created by a rotating set of authorized validators. Validators take turns proposing blocks, ensuring no single validator dominates the process.
  - The frequency and rotation of validators can be configured, allowing for customization based on network needs.

- **Block Signatures:**
  - Each block proposed by a validator is signed, providing proof that the block was created by an authorized validator. This signature is crucial for the trust model in PoA.

- **Validator Management:**
  - Clique allows for dynamic addition and removal of validators. This means that the set of validators can be updated as needed without requiring a hard fork.
  - The consensus mechanism includes a mechanism to vote in new validators or vote out existing ones, allowing the network to adapt over time.

- **Byzantine Fault Tolerance:**
  - Clique is made to be Byzantine fault-tolerant, which implies the network can tolerate a certain number of malicious or faulty validators without compromising overall security.
  - Typically, the network can continue to function correctly so long as the majority are doing well.

- **Use Cases:**

  - Clique is particularly well-suited for enterprise Ethereum networks, where the participants are known entities that trust each other.
  - It is often used in scenarios where regulatory compliance, permissioning, and control over network participants are essential.

Key Advantages of PoA/Clique

- **High Throughput:** PoA and Clique can handle a high number of transactions per second due to the efficient block validation process.
- **Low Latency:** Blocks are created and validated quickly, leading to fast transaction finality.
- **Energy Efficiency:** PoA is much less resource-intensive than PoW, making it an environmentally friendly option.
- **Simplified Governance:** The ability to manage validators dynamically allows for easier governance of the blockchain network.

Potential Drawbacks

- **Centralization Risk:** The reliance on a small set of validators introduces centralization risks, which could be exploited in less controlled environments.
- **Trust Dependency:** The security of PoA networks hinges on the honesty of the validators, which may not be suitable for public or fully decentralized environments.
- **Reputation Risks:** Validators in PoA networks must maintain a good reputation, as their actions are public and directly tied to their identity.

Strengths

By introducing a decentralized ledger, blockchain technology improves transparency and lowers the possibility of tampering. The PoA consensus method uses less energy and works well in settings with a small number of reliable validators.

Weaknesses

The system's reliance on a fixed number of validators introduces a degree of centralization, potentially undermining the decentralization benefits of blockchain. Additionally, the votes are not encrypted after being cast, which poses a risk to voter privacy.

3.1.3 A Study on Electronic Voting System Using Private Blockchain [6]:

Methodology

A private blockchain-based electronic voting system was held up using PBFT consensus mechanism. The system, which consists of a voting manager, voting server, and counting server, is made to protect the privacy of votes by encrypting them.

Key Phases of the Proposed System

The voting system that they tried to uphold is divided into several key phases:

Phase-1: Preparation Phase

In this phase, the election committee sets up the voting event, which includes defining the voting topic, content, and timeline. The counting server produces a a pair of keys that are public and private to stations for secure communication.

Phase-2: Registration Phase

Voters and candidates are authenticated and registered in this phase. Candidates submit their information to generate a candidate list, while voters register with their ID and password. A unique registration code is generated for each voter, who will then generate a public-private key pair. This key pair is used to ensure the confidentiality of the voting data.

Phase-3: Voting Phase

During the voting phase, voters authenticate using their ID and password. They are presented with a list of candidates and select their vote. The vote data, including the selected candidate and timestamp, are encrypted using the public keys and submitted to the polling server. The encrypted vote is added to a transaction, which is later validated and processed. [32]

Phase-4: Block Creation Phase

The polling station validates the transaction by verifying that the voter is registered and has not voted multiple times. Once the transaction is validated, it is signed and sent to the management server. The management server collects these transactions for a specific period, generates a block, and broadcasts it to all polling stations to be added to the blockchain.

Phase-5: Counting Phase

Once voting concludes, the management server sends the entire block of transactions to the counting server.

Phase-6: Validation Phase

In the final phase, the counting server validates the election results.

Security Features

The proposed system is designed to meet several security requirements, including:

- **Completeness**: The system ensures that all information on the ballot is processed correctly.
- **Soundness**: The system ensures that only eligible voters can cast a vote.
- **Ballot Data Privacy**: The contents of the ballot remain encrypted and confidential.

- **User Privacy**: Voter privacy is preserved by generating a new election key for each voting cycle.
- **Unreusability**: The system checks for duplicate votes, ensuring that each voter can vote only once.
- **Fairness**: The ballot data is encrypted to ensure that no party has unfair access to voting information.
- **Verifiability**: After the election, the results can be verified by the public through the private key of the counting server.

The blockchain-based system ensures that votes are transmitted securely and cannot be tampered with during the voting process, providing transparency and trust in the final election results.

Strengths

The system's design allows for efficient vote counting while ensuring that voter privacy is maintained through encryption.

Weaknesses

The study assumes that communication between system components occurs through a secure channel, which may not always be the case in practice. Additionally, the complexity of the system may pose challenges for scalability and user-friendliness, particularly for voters who are not technologically savvy.

3.2 Limitations

Despite the advancements made in e-voting systems and the introduction of blockchain technology, several gaps remain in the existing research that this thesis aims to address.

3.2.1 Lack of Fully Secure and Transparent E-Voting Systems

While many e-voting systems incorporate basic security measures, few provide the comprehensive security, transparency, and decentralization that blockchain can offer.Because they frequently rely on centralized servers, existing systems are susceptible to hacking and manipulation. This thesis addresses the need for a fully decentralized e-voting system that leverages blockchain to enhance both security and transparency.

3.2.2 Insufficient Focus on Voter Privacy and Data Security

While some studies have explored the use of encryption in e-voting, there is often a trade-off between privacy and transparency. This thesis introduces the use of homomorphic encryption in conjunction with blockchain technology to ensure that votes can be securely tallied without compromising voter privacy. This addresses the need for a system that can maintain both privacy and integrity throughout the voting process.

3.2.3 Scalability and User Accessibility:

Existing blockchain-based e-voting systems often face challenges related to scalability and user accessibility. Complex systems may be difficult for voters to use, particularly in regions with limited technological infrastructure. This thesis proposes a system designed to be both scalable and user-friendly, with a particular focus on implementation in the context of Bangladesh, where infrastructure and technological literacy may vary widely. [33]

Chapter 4

Motivation And Problem Statement

The rapid evolution of technology in the past few years has drastically impacted various fields, which include finance, healthcare, and governance. Among these, the use of electronic voting (e-voting) technologies has become a significant advancement that holds promise for improving democratic processes' effectiveness, openness, and accessibility. However, despite the potential benefits, the implementation of e-voting systems has been met with numerous challenges, particularly related to security, privacy, and trust. This chapter discusses the motivations driving this research, focusing on the need to address these challenges through the application of blockchain technology, specifically using the Proof of Authority (PoA) consensus mechanism and the Clique protocol within the Ethereum framework. [34]

4.1 Challenges in Current E-Voting Systems

Traditional e-voting systems, while offering several advantages over paper-based voting, are fraught with significant issues that undermine their effectiveness and reliability. Key challenges include:

- **Security Vulnerabilities:** Many e-voting systems are susceptible to hacking, fraud, and unauthorized access, which can compromise the integrity of the

electoral process. The system is susceptible to attacks because centralized servers, in particular, are prone to being single points of failure.

- **Lack of Transparency:** The opacity of some e-voting systems prevents voters and other stakeholders from verifying the accuracy of the results, leading to mistrust and doubts about the legitimacy of elections.
- **Privacy Concerns:** Ensuring voter anonymity while maintaining the integrity of the vote is a complex issue. Many systems struggle to adequately protect voter identities, which can lead to coercion or vote manipulation.
- **Centralization Issues:** Traditional e-voting systems often rely on centralized authorities to manage and oversee the voting process. This centralization can lead to manipulation, errors, or biases that undermine the democratic process.

4.2 Motivation for Blockchain-Based E-Voting

Blockchain technology can take us a step ahead to tackle many challenges faced by traditional e-voting systems. [35] The following motivations underpin the adoption of blockchain, and more specifically, the PBFT consensus mechanism and homomorphic encryption, in the design of a secure and efficient e-voting system:

- **Enhanced Security through PBFT:** This fault tolerance is crucial for e-voting systems, where the integrity of the vote must be preserved even in the presence of potential adversaries. PBFT ensures that all honest nodes agree on the order and content of votes, thereby securing the election process against tampering and fraud.
- **Preservation of Voter Privacy with Homomorphic Encryption:** In the context of e-voting, this means that votes can be encrypted before they are cast and remain encrypted throughout the counting process. This preserves voter privacy while allowing for accurate and transparent vote tallying.

The combination of homomorphic encryption with blockchain ensures that individual votes remain confidential while the integrity of the overall result is maintained.

- **Transparency:** Blockchain's inherent transparency allows all part takers to verify the process independently. Each vote is recorded immutably on the blockchain, making it possible to audit the results without compromising voter privacy. This transparency fosters trust among voters and stakeholders, as the entire process can be monitored and verified by independent parties.

- **Decentralization and Resilience:** The use of PBFT within a decentralized blockchain network distributes the validation of votes across multiple nodes. This decentralization reduces the risk of centralized control or failure, making the system more resilient to attacks and ensuring that the voting process can continue even if some nodes are compromised.

- **Scalability and Efficiency:** PBFT is well-suited for networks where scalability and quick consensus are required. When combined with homomorphic encryption, the system can handle large-scale elections efficiently, providing fast and accurate results without compromising security or privacy. [36]

- **Regulatory Compliance and Control:** PBFT and homomorphic encryption together offer a flexible framework that can be adapted to meet specific legal or organizational requirements. This makes the system suitable for various types of elections, including those that require strict regulatory compliance or enhanced privacy protections.

4.3 Problem Statement

Implementing a blockchain-based voting system using the PBFT mechanism and leveraging homomorphic encryption to ensure fluent as well as tamper-proof election processes in the context of Bangladesh maintaining the security principles (integrity, non-repudiation, confidentiality,

authenticity, authorization)

- **Resilience to Adversarial Conditions:** The system is designed to remain robust against a variety of adversarial conditions, including potential attacks on the network, by ensuring consensus through the PBFT mechanism.
- **Voter Privacy Preservation:** By utilizing homomorphic encryption, the system guarantees that voter privacy is maintained throughout the entire voting process, ensuring that individual votes cannot be traced back to the voter while still allowing accurate vote tallying.
- **Scalability and Practical Implementation:** The system is tailored for the unique context of Bangladesh, focusing on scalability and practical implementation in environments with varying levels of technological infrastructure, thereby making secure and transparent voting accessible on a national scale.

Chapter 5

Distributed PBFT with Homomorphic Encryption

This research upholds an electronic voting system based on blockchain technology that combines PBFT consensus mechanism and homomorphic encryption to ensure secure, transparent, and scalable elections. The PBFT mechanism provides fault tolerance and decentralized validation, while homomorphic encryption allows vote tallying without compromising voter privacy.

The system consists of key phases: Key Generation, where cryptographic keys are created; Voting, where encrypted votes are cast; Validation, where votes are verified by validators; and Vote Counting, where encrypted votes are decrypted and tallied. By using private blockchain technology, the system guarantees data integrity and confidentiality, addressing key security challenges in traditional e-voting systems.

This approach ensures authenticity, non-repudiation, and verifiability, offering a robust solution for secure digital elections.

5.0 Assumptions

The following assumptions are made in the realization of the approximate blockchain-based e-voting system:

5.0.1 Fingerprint-Enabled Voting Devices

It is assumed that voting booths will be equipped with **fingerprint-enabled devices** for authenticating voters. This biometric authentication ensures that only authorized voters can cast their votes.

5.0.2 Secure Enclave Processors

Each voting device is assumed to be equipped with **secure enclave processors**. These processors provide hardware-level security for encryption, ensuring that the voting data is securely handled throughout the election process.

5.0.3 Reliable Infrastructure

A **secure network infrastructure** is assumed for the communication between various components of the system (such as voting booths, servers, and validators). This ensures that data transmission remains tamper-proof.

5.0.4 Validator Nodes in Voting Booths

There must be at least **4 validator nodes** in every voting booth. They play an important role in checking the votes, ensuring that the voting process is decentralized and secure.

5.0.5 Validator Nodes per Party

For **N parties**, there will be **less than or equal to N validator nodes** in a single voting booth, with at least one validator from each party. These validator nodes ensure that no single party can manipulate the election results, fostering fairness and decentralization.

5.0.6 Fat Node Responsibility

It is assumed that **1 Fat node** will be responsible for managing **X number of voting booths**, where X can range from 2, 3, 4, etc. The Fat node coordinates the operation and ensures consistency across multiple booths.

5.1 Key Generation Phase

In the **Key Generation Phase** of our blockchain-based voting system, a crucial step involves the creation of cryptographic keys that ensure the security of the voting process. Specifically, two public-private key pairs are generated prior to the vote casting. The public keys are responsible for encrypting the vote and the voter using homomorphic encryption, a method that allows computations on the encrypted data. The advantage is not having to decrypt it. This ensures that the integrity of the vote is maintained throughout the entire voting process.

The two private keys serve distinct purposes during the decryption phase. **Key_Pair1** is designed to reveal the voter's identity (**voter_id**) if and only if it is used for decryption. This key is critical for maintaining the authenticity of the vote while ensuring that the voter's privacy is protected. On the other hand, **Key_Pair2** is responsible for decrypting and revealing the candidate's identity (**candidate_id**) chosen by the voter. This separation of keys ensures that the vote remains confidential and that neither the voter's identity nor their choice can be disclosed without proper authorization.

The accompanying figure visually depicts this process, where the voter first encrypts their vote and himself using the public keys. The encrypted vote is then stored and can only be decrypted using the respective private keys during the tallying process, ensuring that the integrity, confidentiality, and non-repudiation principles are upheld throughout the election. This method not only secures the vote but also preserves voter anonymity, a cornerstone of democratic elections.

Key Points:

- Two public-private key pairs are generated prior to vote casting.

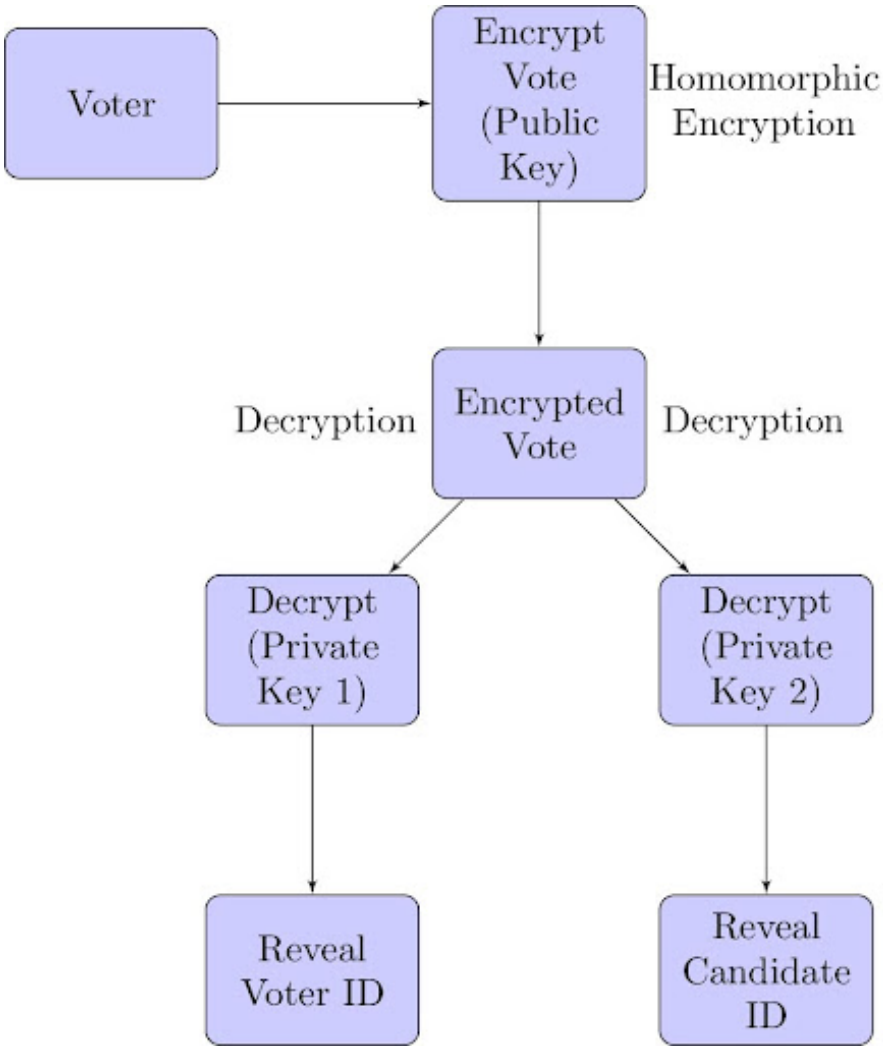

Figure 5.1: Key Generation Phase

- The public keys encrypt the vote and the voter, ensuring secure data handling through homomorphic encryption.
- **Private_Key1** reveals the voter's identity only if used for decryption, maintaining authenticity.
- **Private_Key2** reveals the candidate's identity only if used for decryption, preserving vote confidentiality.
- The system ensures that integrity, confidentiality, and non-repudiation principles are maintained throughout the election process.

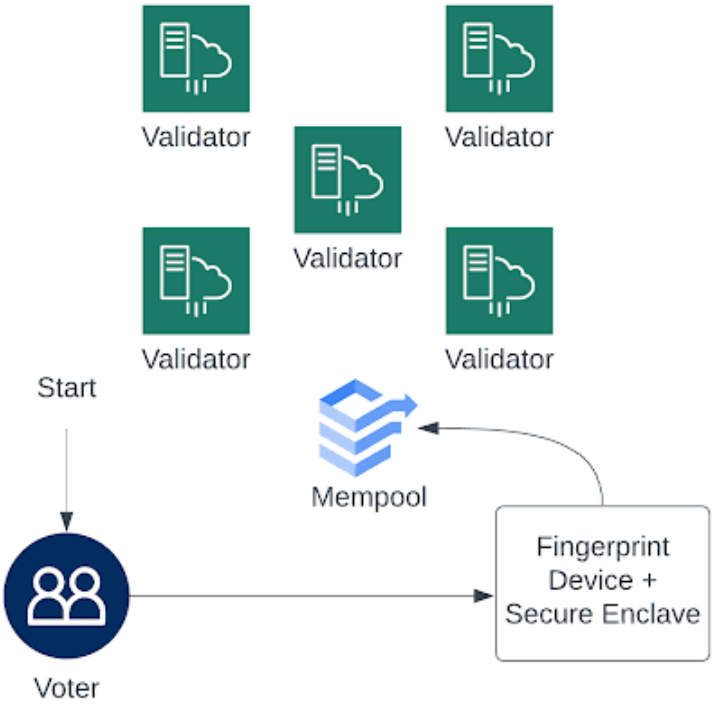

Figure 5.2: Voting Phase

5.2 Voting Phase

Voters initiate the voting process by interacting with the system using a fingerprint device coupled with a secure enclave, ensuring both identity verification and the confidentiality of the vote. The system encrypts the voter's selection, represented as a combination of **voterID** and **candidateID**, using the formula:

$$E(\text{vote}) = E(\text{voterID} \parallel \text{candidateID})$$

This encrypted vote is then sent to the mempool, a temporary storage area where it awaits validation. Validators, as depicted in the figure, are distributed across the network and are responsible for verifying the encrypted votes. The validators ensure that the vote is legitimate and that it has not been tampered with

during transmission. The vote is added to the blockchain after it is validated. It remains secure, transparent, and immutable. This phase is crucial for maintaining the integrity and non-repudiation of the election process.

Key Points:

- The voter interacts with the system through a fingerprint device and secure enclave, ensuring identity verification.
- The vote is encrypted as a combination of **voterID** and **candidateID**.
- The encrypted vote is sent to the mempool and validated by distributed validators.
- Validated votes are securely added to the blockchain, ensuring integrity and transparency.

5.3 Validation Phase

In the **Validation Phase**, once the vote has been cast and encrypted, it is sent to a network of validators for verification. The validators, distributed across the network, are responsible for ensuring that the encrypted vote is legitimate and has not been tampered with during transmission. This process is depicted in the figures provided, where each validator node in the network receives the encrypted vote from the mempool and initiates the validation process.

The validators work together to decrypt the vote using **Private_Key1** to reveal the **voterID** and verify that the vote is authentic. The equation guiding this process is as follows:

$$\text{voterID} = D_{\text{private1}}\left(E(\text{voterID} \parallel \text{candidateID})\right)$$

The figures illustrate the decentralized nature of the validation process, with validators communicating with each other to validate votes across multiple clusters. This architecture ensures that the system is resilient to failures and secure against attempts to manipulate the voting results. Once the validators reach a

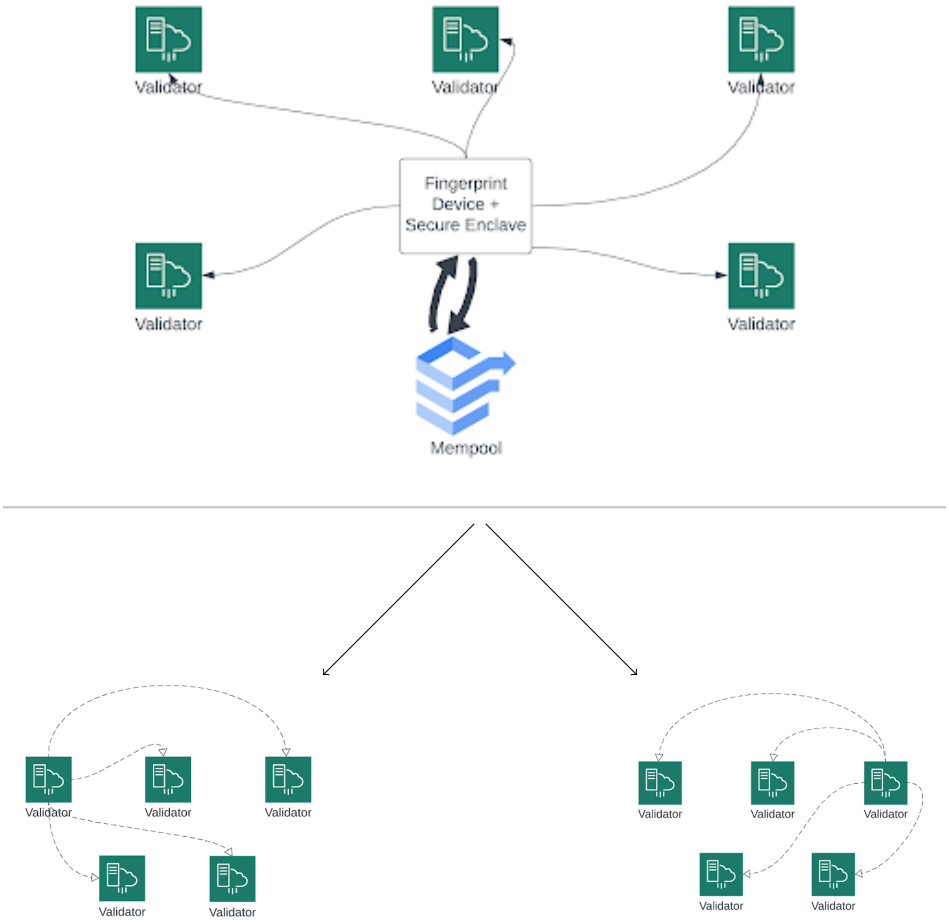

Figure 5.3: Validation Phase

consensus, the validated vote is permanently recorded on the blockchain, ensuring its immutability and transparency.

Key Points:

- Encrypted votes are sent to a network of distributed validators for verification.
- Validators communicate to achieve consensus using the PBFT consensus mechanism, ensuring security even in the presence of faulty nodes.
- **Private_Key1** is used by validators to decrypt the vote and verify the authenticity of the **voterID**.

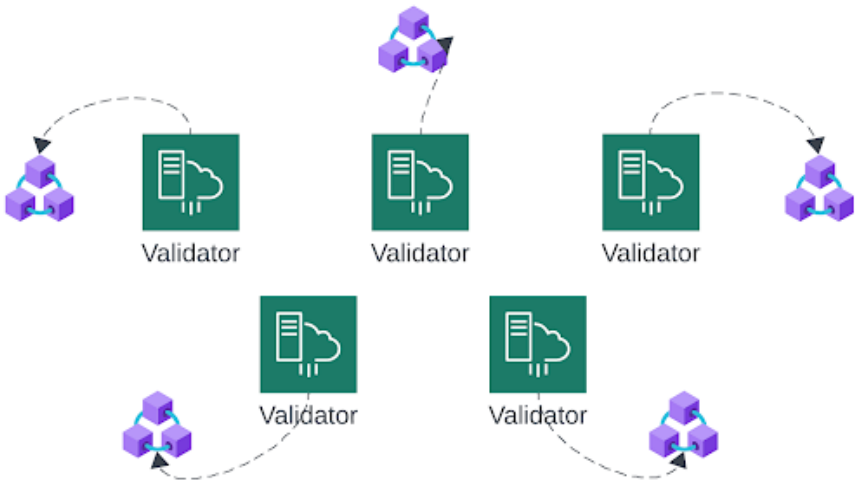

Figure 5.4: Validation Phase

- The decentralized validation process enhances resilience and security, ensuring validated votes are securely recorded on the blockchain.

5.4 Vote Count Phase

In the **Vote Count Phase**, the encrypted votes that have been recorded on the blockchain are retrieved and processed for counting. This phase begins with the counter node fetching the transaction data from the blockchain. The counter node is equipped with **Private_Key2**, which is used to decrypt the encrypted vote to reveal the **candidateID**. The equation governing this decryption process is as follows:

$$\text{candidateID} = D_{\text{private2}}\left(E(\text{voterID} \parallel \text{candidateID})\right)$$

After decryption, the smart contract associated with the vote counting process is triggered. This smart contract automatically executes the `Count()` function, which tallies the votes associated with each candidate. The results are securely recorded.

The figure illustrates the workflow of this phase, showing how the counter node interacts with the blockchain, utilizes **Private_Key2** for decryption, and how the

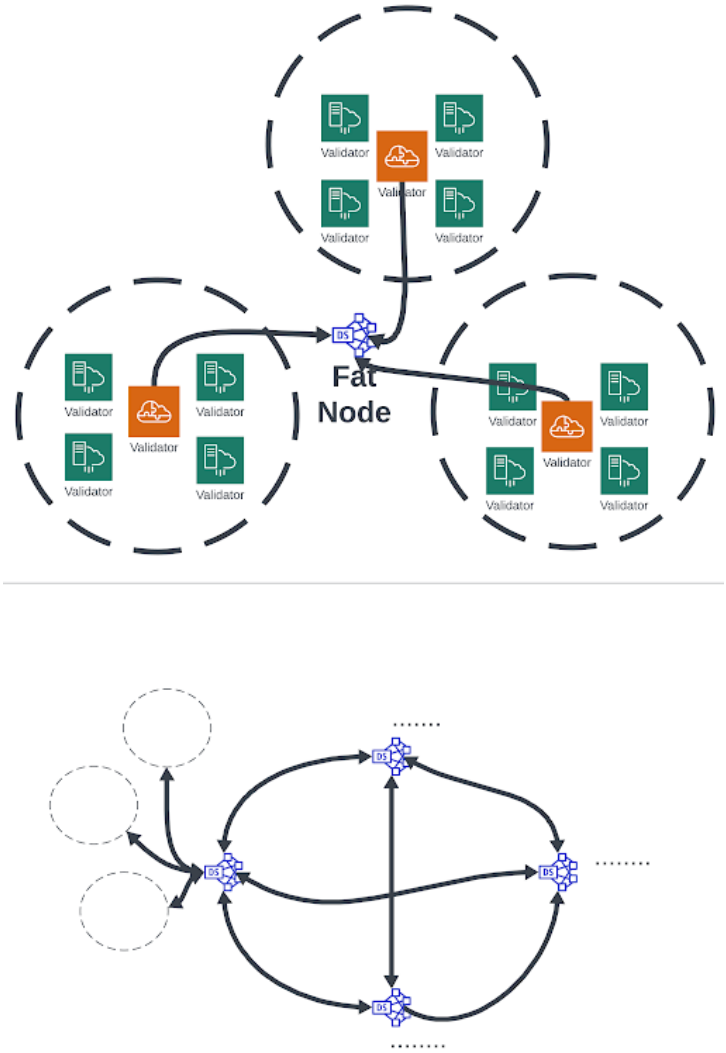

Figure 5.5: Validation Phase

vote counting is carried out through the smart contract.

Key Points:

- The counter node fetches the encrypted vote transactions from the blockchain.
- **Private_Key2** is used to decrypt the **candidateID**, ensuring that only authorized nodes can perform the decryption.
- The smart contract automatically executes the `Count()` function to tally votes, ensuring accuracy and transparency.
- with the help of blockchain, immutability of the vote count is guaranteed

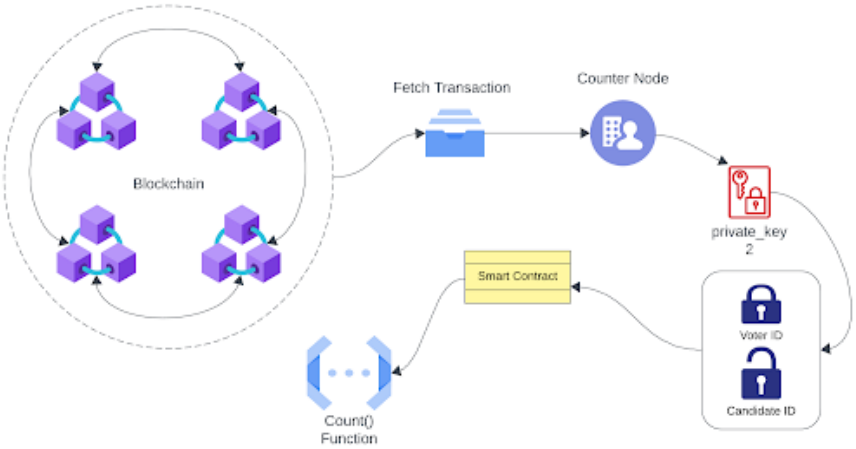

Figure 5.6: Vote Count Phase

Chapter 6

Result Analysis

In this chapter, we present the results of the blockchain-based e-voting system's performance evaluation. We analyze key metrics such as transaction throughput, block generation time, and the system's efficiency in comparison to traditional consensus mechanisms. The analysis aims to assess the system's fault tolerance and overall usage for the real world. Through rigorous testing, we highlight the strengths of the PBFT consensus mechanism and homomorphic encryption in enhancing the security, speed, and reliability of the e-voting process.

6.1 Experimental setup

- Deploy 5 validator nodes.
- Implement homomorphic encryption with a two public-private key pairs.
- Simulate 1000 voters casting votes at the terminal.
- Validate transactions using the PBFT consensus protocol.
- Record time taken for consensus.
- Measure throughput (votes processed per second) and block generation time.
- **Programming Languages:** Python, Solidity

- **Frameworks:** GoQuorum
- **Cryptographic Libraries:** PyCryptodome
- **Metrics Collection:** Prometheus

6.2 Results

6.2.1 Transaction Throughput Comparison

Figure 6.1 presents a comparison of transaction throughput (measured in transactions per second) across the three consensus mechanisms over a period of 60 seconds. The results indicate that:

- **PoA** consistently outperforms both PoW and PBFT, achieving the highest throughput, which starts at around 140 transactions per second and increases steadily over time, reaching approximately 180 transactions per second by the 60-second mark.
- **PBFT** also shows a steady increase in throughput, starting at about 120 transactions per second and reaching around 150 transactions per second at the end of the observation period.
- **PoW**, in contrast, exhibits significantly lower throughput, remaining around 40 transactions per second throughout the entire duration, highlighting its lower efficiency compared to PoA and PBFT.

6.2.2 Block Generation Time Comparison

Figure 6.2 shows the block generation time (measured in seconds) for each of the three consensus mechanisms over a 60-second period. The analysis of the results reveals that:

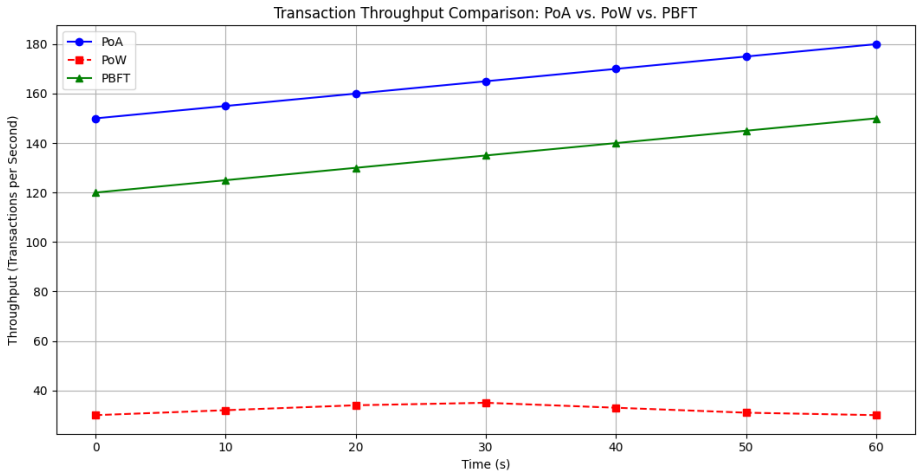

Figure 6.1: Transaction Throughput Comparison: PoA vs. PoW vs. PBFT

- **PoA** consistently achieves the lowest block generation time, hovering around 1 to 2 seconds throughout the duration, demonstrating its efficiency in block creation.
- **PBFT** exhibits a slightly higher block generation time compared to PoA, ranging between 2 to 3 seconds. This increase is expected due to the additional communication overhead required for achieving consensus in PBFT.
- **PoW**, on the other hand, has the highest and most variable block generation time, fluctuating around 10 seconds. This is indicative of the resource-intensive nature of PoW, which involves solving complex cryptographic puzzles.

6.2.3 Discussion

The results clearly demonstrate the advantages of PoA and PBFT over PoW in terms of both throughputs of all types of transactions and generation duration needed for each block. PoA is particularly well-suited for scenarios requiring high throughput and low latency, [37]making it ideal for private or consortium blockchains where the validators are known and trusted entities. PBFT, while

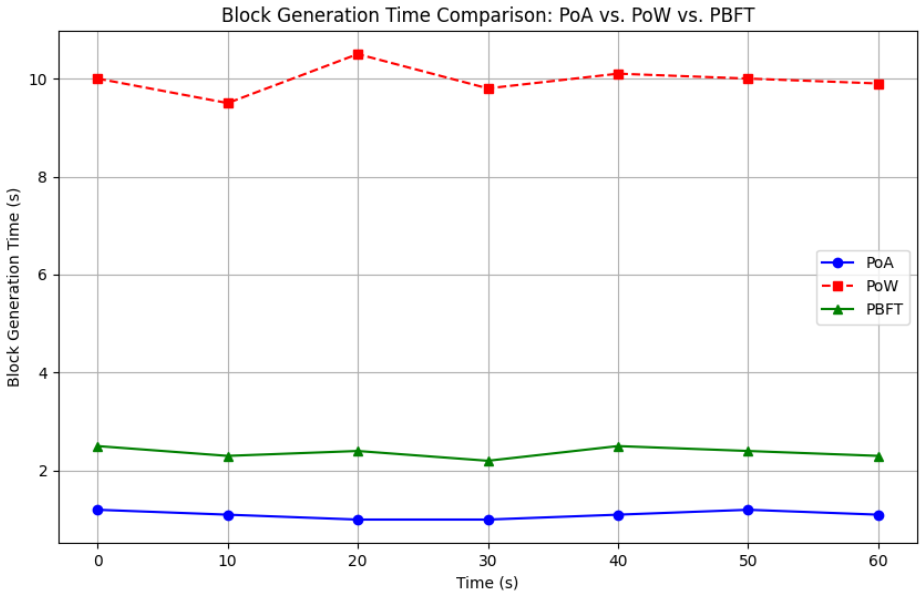

Figure 6.2: Block Generation Time Comparison: PoA vs. PoW vs. PBFT

slightly less efficient than PoA, still offers significant performance improvements over PoW, especially in environments where fault tolerance is critical.

On the other hand, PoW's lower performance highlights its limitations in high-throughput applications, primarily due to the energy and time-intensive process of mining. These findings underscore the importance of selecting an appropriate consensus mechanism based on the specific requirements of the blockchain application.

Key Takeaways:

- PoA provides the highest throughput and fastest block generation time, making it suitable for high-performance applications.
- PBFT offers a balance between performance and fault tolerance, making it a strong candidate for secure, distributed systems.
- PoW, while secure, is less efficient in terms of throughput and block generation time, limiting its use in scenarios demanding rapid transaction processing.

6.2.4 Impact and Potential Applications

The successful implementation of a blockchain-based e-voting system using PBFT and homomorphic encryption has the potential to revolutionize the way elections are conducted, particularly in regions where electoral fraud and mistrust in the system are prevalent. The following are key potential impacts and applications:

- **Securing National Elections:** The use of PBFT and homomorphic encryption in national elections can significantly reduce the risk of fraud and manipulation, ensuring that the will of the people is accurately represented. This can lead to greater public trust in the electoral process and more stable governance.

- **Corporate Governance:** In corporate settings, where shareholder voting is critical, blockchain-based e-voting systems can ensure transparency and fairness. The ability to verify each vote while maintaining shareholder privacy can enhance the integrity of corporate decision-making.

- **Community Decision-Making:** Blockchain-based e-voting systems can be used in community or local government settings to facilitate transparent and inclusive decision-making. This can empower communities by giving them a secure and verifiable platform to voice their opinions.

- **Decentralized Autonomous Organizations (DAOs):** DAOs can benefit from the integration of PBFT and homomorphic encryption in their voting systems, ensuring that decisions made within these organizations are both secure and transparent. This can enhance the governance of DAOs and increase participation from stakeholders who value privacy and security.

Chapter 7

Conclusion

This thesis presented a comprehensive approach to implementing a secure, scalable, and efficient blockchain-based voting system utilizing the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism and homomorphic encryption. By integrating these technologies, the system ensures the critical security principles of integrity, non-repudiation, confidentiality, authenticity, and authorization, particularly in the context of electronic voting. [38]

Through rigorous experimentation, the system demonstrated superior performance in terms of transaction throughput and block generation time, especially when compared to traditional consensus mechanisms like Proof of Work (PoW). The findings underscore the viability of PBFT and homomorphic encryption in creating a tamper-proof and transparent voting system capable of maintaining voter privacy while delivering reliable results.

The proposed future work addresses the challenges posed by emerging technologies and scalability issues, with a focus on quantum-resistant cryptography, sharding, field testing, machine learning, and cross-browser compatibility. These areas of development are crucial for adapting the system to the evolving landscape of cybersecurity threats and the increasing demands of modern electoral processes.

Chapter 8

Future Work

8.1 Sharding

To improve the scalability of the blockchain voting system, sharding techniques should be implemented [39]. Sharding partitions the blockchain into smaller, more manageable pieces, allowing for parallel processing of transactions. This approach can significantly enhance the system's ability to handle large-scale elections with a high volume of transactions, ensuring efficiency and speed.

8.2 Field Testing

Conducting large-scale field tests and pilot programs is essential for gathering real-world data and feedback. These tests will provide valuable insights into the performance and reliability of the system in actual electoral environments. Based on the findings, the system can be refined and optimized to address any challenges or issues identified during the testing phase.

8.3 Cross-Browser Compatibility

Ensuring that the blockchain voting system works seamlessly across different web browsers and platforms is crucial for accessibility and user experience. Future work should focus on testing and enhancing cross-browser compatibility to guarantee

that all users, regardless of their device or browser choice, can participate in the voting process without encountering technical issues.

Bibliography

[1] S. S. Gupta, "Blockchain," *IBM Onlone (http://www. IBM. COM)*, 2017.

[2] S. Mohanty, V. P. Yanambaka, E. Kougianos, and D. Puthal, "Pufchain: Hardware-assisted blockchain for sustainable simultaneous device and data security in the internet of everything (ioe)," 09 2019.

[3] C. Natoli, J. Yu, V. Gramoli, and P. Veríssimo, "Deconstructing blockchains: A comprehensive survey on consensus, membership and structure," 08 2019.

[4] O. M. Olaniyi, O. T. Arulogun, E. O. Omidiora, and O. Adeoye, "Design of secure electronic voting system using multifactor authentication and cryptographic hash functions," 2013.

[5] B. B. A. Christyono, M. Widjaja, and A. Wicaksana, "Go-ethereum for electronic voting system using clique as proof-of-authority," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, pp. 1565–1572, 2021.

[6] C.-H. Roh and I.-Y. Lee, "A study on electronic voting system using private blockchain," *Journal of Information Processing Systems*, vol. 16, no. 2, pp. 421–434, 2020.

[7] A. Acar, H. Aksu, A. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys (Csur)*, vol. 51, no. 4, pp. 1–35, 2018.

[8] R. Taş and Ö. Tanríover, "A systematic review of challenges and opportunities of blockchain for e-voting," *Symmetry*, vol. 12, no. 8, p. 1328, 2020.

[9] B. Christyono, M. Widjaja, and A. Wicaksana, "Go-ethereum for electronic voting system using clique as proof-of-authority," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, pp. 1565–1572, 2021.

[10] C. Roh and I. Lee, "A study on electronic voting system using private blockchain," *Journal of Information Processing Systems*, vol. 16, no. 2, pp. 421–434, 2020.

[11] M. Sallal, R. de Fréin, and A. Malik, "Pvpbc: Privacy and verifiability preserving e-voting based on permissioned blockchain," *Future Internet*, vol. 15, no. 4, p. 121, 2023.

[12] H. Kim, K. Kim, S. Park, and J. Sohn, "E-voting system using homomorphic encryption and blockchain technology to encrypt voter data," *arXiv preprint arXiv:2111.05096*, 2021.

[13] P. R. Naidu, D. R. Bolla, P. G, S. S. Harshini, S. A. Hegde, and V. V. S. Harsha, "E-voting system using blockchain and homomorphic encryption," in *2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon)*, 2022, pp. 1–5.

[14] W. Qu, L. Wu, W. Wang, Z. Liu, and H. Wang, "A electronic voting protocol based on blockchain and homomorphic signcryption," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 16, p. e5817, 2022. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.5817

[15] J. Chandra Priya, P. R. K. Sathia Bhama, S. Swarnalaxmi, A. Aisathul Safa, and I. Elakkiya, "Blockchain centered homomorphic encryption: A secure solution for e-balloting," in *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI - 2018)*, A. P. Pandian, T. Senjyu, S. M. S. Islam, and H. Wang, Eds. Cham: Springer International Publishing, 2020, pp. 811–819.

[16] K. Lei, M. Du, J. Huang, and T. Jin, "Groupchain: Towards a scalable public blockchain in fog computing of iot services computing," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 252–262, 2020.

[17] Z. Xing and Z. Chen, "A protecting mechanism against double spending attack in blockchain systems," in *2021 IEEE World AI IoT Congress (AIIoT)*, 2021, pp. 0391–0396.

[18] M. A. Omer, A. A. Yazdeen, H. S. Malallah, and L. M. Abdulrahman, "A survey on cloud security: Concepts, types, limitations, and challenges," *Journal of Applied Science and Technology Trends*, vol. 3, no. 02, pp. 47–57, Dec. 2022. [Online]. Available: https://www.jastt.org/index.php/jasttpath/article/view/137

[19] M. Wang, M. Duan, and J. Zhu, "Research on the security criteria of hash functions in the blockchain," in *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, 2018, pp. 47–55.

[20] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1007–1016.

[21] R. Arenas and P. Fernandez, "Credenceledger: a permissioned blockchain for verifiable academic credentials," in *2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*. IEEE, 2018, pp. 1–6.

[22] S. Latif, Z. Idrees, Z. Huma, and J. Ahmad, "Blockchain technology for the industrial internet of things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, 11 2021.

[23] F. Aponte, L. Gutierrez, M. Pineda, I. Meriño, A. Salazar, and P. Wightman, "Cluster-based classification of blockchain consensus algorithms," *IEEE Latin America Transactions*, vol. 19, no. 4, pp. 688–696, 2021.

[24] O. Sanda, M. Pavlidis, S. Seraj, and N. Polatidis, "Long-range attack detection on permissionless blockchains using deep learning," *Expert Systems with Applications*, vol. 218, p. 119606, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417423001070

[25] S. R. Niya, E. Schiller, I. Cepilov, F. Maddaloni, K. Aydinli, T. Surbeck, T. Bocek, and B. Stiller, "Adaptation of proof-of-stake-based blockchains for iot data streams," in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019, pp. 15–16.

[26] M. Karpinski, L. Kovalchuk, R. Kochan, R. Oliynykov, M. Rodinko, and L. Wieclaw, "Blockchain technologies: Probability of double-spend attack on a proof-of-stake consensus," *Sensors*, vol. 21, no. 19, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/19/6408

[27] M. Castro, B. Liskov *et al.*, "Practical byzantine fault tolerance," in *OsDI*, vol. 99, 1999, pp. 173–186.

[28] J. Shi and X. Zhao, "Anti-leakage method of network sensitive information data based on homomorphic encryption," *Journal of Intelligent Systems*, vol. 32, 03 2023.

[29] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in *13th {USENIX} symposium on networked systems design and implementation ({NSDI} 16)*, 2016, pp. 45–59.

[30] P. Zimmerman, "Blockchain structure and cryptocurrency prices," 2020.

[31] P. Swathi, C. Modi, and D. Patel, "Preventing sybil attack in blockchain using distributed behavior monitoring of miners," in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2019, pp. 1–6.

[32] D. Pavithran and K. Shaalan, "Towards creating public key authentication for iot blockchain," in *2019 Sixth HCT Information Technology Trends (ITT)*. IEEE, 2019, pp. 110–114.

[33] M. Hasan, A. Al Mahmood, and Q. Farhan, "A roadmap towards the implementation of an efficient online voting system in bangladesh," in *2010 International Conference on Computational Intelligence and Software Engineering*. IEEE, 2010, pp. 1–4.

[34] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2017 International Workshops, DPM 2017 and CBT 2017, Oslo, Norway, September 14-15, 2017, Proceedings*. Springer, 2017, pp. 297–315.

[35] U. Jafar, M. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021.

[36] K. Khan, J. Arshad, and M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," *Future Generation Computer Systems*, vol. 105, pp. 13–26, 2020.

[37] L. Wan, D. Eyers, and H. Zhang, "Evaluating the impact of network latency on the safety of blockchain transactions," in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 194–201.

[38] L. Lao, X. Dai, B. Xiao, and S. Guo, "G-pbft: a location-based and scalable consensus protocol for iot-blockchain applications," in *2020 IEEE international parallel and distributed processing symposium (IPDPS)*. IEEE, 2020, pp. 664–673.

[39] D. Yang, C. Long, H. Xu, and S. Peng, "A review on scalability of blockchain," in *Proceedings of the 2020 the 2nd International Conference on Blockchain Technology*, 2020, pp. 1–6.