Research Project Proposal

Final Year

Blockchain-based E-voting System

Group 08

E/19/193	Kaushalya N. V. K.
E/19/363	Senevirathne T. N.
E/19/375	Silva N. H. D. U

Department of Computer Engineering

Faculty of Engineering

University of Peradeniya

2025

Research Project Proposal

Final Year

Blockchain-based E-voting System

Group 08

E/19/193 Kaushalya N. V. K.

E/19/363 Senevirathne T. N.

E/19/375 Silva N. H. D. U

Supervised by : Prof. Manjula Sandirigama

Department of Computer Engineering

Faculty of Engineering

University of Peradeniya

2025

Abstract

Traditional paper-based voting systems face challenges related to security, privacy, efficiency, and fairness, including risks of fraud, human error, and logistical inefficiencies. Although electronic and internet-based voting systems were introduced to address these issues, they introduced new vulnerabilities such as cybersecurity threats, lack of voter verifiability, and privacy concerns. To overcome these challenges, this research proposes the design and implementation of a secure, scalable, and transparent e-voting system using blockchain technology.

The system aims to maintain the integrity of each vote, prevent tampering, protect voter privacy, and ensure consistent performance. Specific objectives include preventing manipulation, investigating scalability solutions, enhancing coercion resistance through anonymous voting and secure authentication, automating voting rules with smart contracts, and improving user-friendliness to foster broader participation and trust.

The proposed methodology consists of five phases: voter registration, candidate registration, voting, vote counting, and result announcing phase. In the voter registration phase, voters receive secret keys through the post and at the polling station, which are combined to generate a voting key for secure authentication. The candidate registration phase involves verifying eligibility and securely storing candidate information on the blockchain. During the voting phase, voters cast their votes at polling stations and immediately verify them on-screen. Finally, votes are counted, and the result is announced.

This research leverages blockchain's decentralized and immutable nature to provide a secure and verifiable voting solution while addressing challenges related to scalability, privacy, and coercion resistance. By enhancing security, transparency, and user-friendliness, the proposed system aims to restore trust and confidence in the electoral process.

Table of Contents

List of Figures

List of tables

Chapter 01

Introduction

1.1 Introduction

Voting is a cornerstone of democracy, allowing citizens to actively participate in governance and decision-making processes. As societies progress, the methods of casting ballots have also evolved. From traditional paper-based voting to electronic voting (e-voting) and, more recently, internet-based voting (I-voting), these advancements aim to improve efficiency, accessibility, and the speed of election results. However, these changes also bring increased complexity in ensuring that the voting process remains secure, transparent, and trustworthy.

1.2 E-voting and I-voting Overview

E-voting systems use electronic devices, such as voting machines or kiosks, to record votes, offering a faster and more efficient process compared to traditional manual counting. These systems have been implemented in various elections worldwide, promising a reduction in human error and quicker tallying of results.

I-voting, or internet-based voting, allows citizens to cast their votes via the internet, providing enhanced accessibility, particularly for voters unable to attend physical polling stations. This system aims to make voting more inclusive by overcoming geographical and physical barriers and offering a more convenient voting experience.

1.3 Challenges in E-voting and I-voting

While e-voting and I-voting bring numerous advantages, they also introduce new challenges. Cybersecurity risks, software vulnerabilities, and the importance of safeguarding privacy and vote integrity are critical considerations in the transition to

digital elections. Ensuring that the voting system remains tamper-proof and verifiable is essential for maintaining trust and integrity in the electoral process.

1.4 Blockchain and Its Role in Enhancing Voting System

Blockchain, a decentralized and tamper-resistant digital ledger, has emerged as a promising solution to enhance the security, transparency, and verifiability of voting systems. Known for its ability to securely record and store digital transactions, blockchain can be used to ensure that votes are cast, recorded, and stored immutably, reducing the possibility of tampering or fraud.

Smart contracts, self-executing contracts with terms directly written into code, offer an additional layer of automation for blockchain-based voting systems. These contracts can manage various aspects of the voting process, such as voter identity verification, ensuring eligibility, and vote tallying. This automation not only reduces the risk of human error but also minimizes the chances of fraud, contributing to a more secure election process.

1.5 Global Voting Methods

Different electoral systems are used worldwide to ensure fair representation of voter preferences. Notable methods include:

- First Past the Post (FPTP): Used predominantly in countries like the US and UK, FPTP gives victory to the candidate with the most votes in a constituency, even without a majority. While simple, this method can lead to disproportional outcomes.

- Instant Run-off Voting (IRV): IRV allows voters to rank candidates. If no candidate wins a majority in the first round, the lowest-ranking candidate is

eliminated, and their votes are redistributed until a candidate achieves a majority.

- Two-Round Run-off: Used in countries like France, this method holds a second round between the top two candidates if no majority is reached in the first round.

- Proportional Representation (PR): PR allocates seats based on the percentage of votes received by each party or candidate. This system ensures a fairer representation, especially for smaller parties, as opposed to FPTP, which can overrepresent larger parties.

For this implementation, we will use the Instant Run-off Voting (IRV) method, as it aligns with the system used for presidential elections in Sri Lanka.

1.6 Future of Blockchain in Voting

Despite the promising potential of blockchain technology, several challenges must be addressed before it can be widely adopted in voting systems. These include scalability issues, regulatory concerns, and ensuring user accessibility. However, blockchain holds the promise of revolutionizing the electoral process by creating a more secure, transparent, and efficient system that could redefine how elections are conducted in the future.

1.7 Problem Statement

Voting is one of the most fundamental pillars of democracy, granting citizens the ability to express their opinions, choose their representatives, and influence the policies that shape their nation's future. A fair, transparent, and secure voting system is essential to uphold democratic principles and ensure that the electoral process accurately reflects the will of the people. However, traditional paper-based voting methods have long faced significant challenges related to security, privacy, efficiency, and fairness. Since these

systems rely on a centralized authority to manage and oversee elections, they remain susceptible to various risks, including fraud, human error, manipulation, and logistical inefficiencies. Ballots can be lost, miscounted, or even deliberately tampered with, leading to disputes over election results and a loss of public confidence in the democratic process. These limitations highlight the urgent need for a more secure, transparent, and tamper-resistant voting system.

To address the challenges posed by paper-based voting, electronic and internet-based voting systems were introduced to improve efficiency, accessibility, and accuracy. These digital voting methods eliminated some of the logistical challenges of traditional voting, such as manual vote counting and physical storage of ballots. However, they introduced new risks and vulnerabilities that threatened the integrity of elections. Cybersecurity threats, such as hacking, malware attacks, vote tampering, and system failures, have raised serious concerns regarding the reliability of electronic voting. Additionally, many e-voting systems fail to provide adequate voter verifiability and transparency, making it difficult for individuals to independently confirm that their votes were recorded and counted correctly. Furthermore, privacy concerns remain unresolved, as some systems expose sensitive voter data, making them susceptible to surveillance or coercion.

A truly secure and reliable voting system must address the shortcomings of both traditional and electronic voting while ensuring the fundamental principles of democracy are upheld. This requires a system that balances security, transparency, voter privacy, verifiability, scalability, and fairness. The key challenge lies in developing a solution that not only prevents fraud and manipulation but also maintains voter confidence in the process. To achieve this, there is a growing need for innovative technologies capable of providing a verifiable, tamper-proof, and decentralized election system.

One of the most promising solutions to these challenges is blockchain technology, which offers a secure and transparent method for recording and verifying transactions in a decentralized manner. By leveraging blockchain, voting systems can ensure immutability, auditability, and enhanced security while preserving voter privacy. The decentralized nature of blockchain eliminates the reliance on a single authority, reducing

the risks of manipulation or tampering. Additionally, cryptographic techniques such as zero-knowledge proofs [16], threshold cryptography, homomorphic encryption, and digital signatures can be integrated into blockchain-based voting to further strengthen anonymity, authentication, and vote integrity.

As governments and organizations worldwide seek to modernize election processes, it is crucial to explore how blockchain technology can be effectively implemented to enhance the security, trust, and transparency of electronic voting. The success of such a system will depend on its ability to address key challenges such as ballot secrecy, voter verifiability, coercion resistance, scalability, legal compliance, and accessibility. Through continuous research and development, blockchain-based voting solutions have the potential to revolutionize electoral systems, paving the way for a more secure, transparent, and reliable voting process that upholds the true essence of democracy.

1.8 Aim and Objectives

The research Aim and objectives are listed below.

1.8.1. Aim

The primary aim of this research is to thoroughly investigate how blockchain technology can be effectively utilized to enhance the security, trust, transparency, and overall integrity of electronic voting systems. Traditional voting methods, including both paper-based and electronic systems, have been plagued by various challenges that threaten the credibility and fairness of elections. Issues such as vote manipulation, lack of transparency, inefficiencies in vote counting, multiple voting, coercion, voter privacy concerns, and centralization risks have long been present in conventional voting mechanisms. These challenges often result in electoral disputes, loss of public confidence, and potential interference in democratic processes. Therefore, there is a strong need for a secure, verifiable, and tamper-resistant voting system that ensures every vote is accurately recorded, stored, and counted without external interference.

This study aims to design and develop a blockchain-based voting framework that upholds key democratic principles such as ballot secrecy, voter verifiability, contestability, and auditability while maintaining efficiency, accessibility, and fairness. Blockchain technology, with its decentralized, immutable, and transparent nature, presents an innovative solution to the vulnerabilities of both traditional and electronic voting systems. By integrating advanced cryptographic techniques such as zero-knowledge proofs, threshold cryptography, digital signatures, and homomorphic encryption, the goal is to establish a voting system that guarantees privacy, security, and fraud resistance while enabling voters to verify their ballots without compromising anonymity.

Furthermore, this research seeks to evaluate the feasibility of real-world implementation of blockchain-based voting by ensuring that the system is scalable, cost-effective, transparent, secure, coercion-resistant, accessible, and legally compliant. The study will assess how blockchain networks, including public, private, and hybrid models [7, 11], can be adapted to different electoral processes while maintaining high standards of data integrity, reliability, and efficiency. The research will also explore how smart contracts and consensus mechanisms can be leveraged to automate election procedures, minimize human intervention, and enhance overall security. [12]. Table 1.1 compares and contrasts some of the different consensus mechanisms [33].

Additionally, the study aims to address key challenges such as voter coercion, system vulnerabilities, usability, legal considerations, and verification difficulties, ensuring that the proposed solution is universally adaptable for both small-scale and large-scale elections. By systematically analyzing these aspects, this research aspires to contribute to the development of a trustworthy, auditable, and resilient electronic voting system that can be integrated into modern electoral frameworks, ultimately strengthening democracy and public confidence in election outcomes. [28]

Table 1.1: Blockchain consensus mechanisms comparison

Consensus Mechanism	Security	Scalability	Energy Usage	Examples
Proof of Work (PoW)	High	Low	High	Bitcoin, Ethereum
Proof of Stake (PoS)	Medium	High	Low	Ethereum 2.0, Cardano
Proof of Authority (PoA)	Medium	High	Low	Binance Smart Chain
Proof of Elapsed Time (PoET)	Medium	High	Low	Hyperledger
Proof of Burn (PoB)	High	Medium	Medium	Slimcoin

1.8.2. Objectives

- General Objective:

  To design and implement a secure, scalable, and transparent e-voting system that ensures the integrity of each vote, prevents tampering, and protects voter privacy. The system will incorporate mechanisms to accurately record and safeguard all votes, ensuring they remain free from unauthorized alterations or deletions. Emphasis will be placed on scalability, with strategies to handle high voter traffic, optimize resource allocation, and maintain consistent performance during peak periods [13]. Methods for coercion

resistance will also be explored to prevent external pressures or manipulation, utilizing anonymous voting mechanisms and secure authentication to protect voter autonomy and privacy. Additionally, automated voting rules will be enforced through smart contracts to consistently apply predefined policies, reducing the likelihood of errors or manual manipulation. Finally, the system will prioritize user-friendliness by designing intuitive interfaces and simplifying the voting process for all users, ensuring easy navigation, clear instructions, and robust security. This comprehensive approach aims to foster trust and confidence in the overall election process [2],[4].

- Specific objectives:
    1. To ensure that the voting process is protected from tampering or manipulation: The objective is to maintain the integrity of each vote, ensuring accurate recording and safeguarding of all votes. This approach focuses on creating a transparent and reliable voting environment where voters' choices are preserved without unauthorized alterations or deletions. By doing so, it fosters trust and confidence in the overall election process.

    2. To investigate scalability: [8] The focus is on exploring methods to ensure the system can handle high voter traffic without compromising speed or accuracy. This involves identifying and addressing potential bottlenecks, optimizing resource allocation, and ensuring consistent performance even during peak voting periods. By enhancing scalability, the system can accommodate larger numbers of voters while maintaining reliability, responsiveness, and data integrity throughout the voting process. [27]

    3. To explore more on how to prevent coercion resistance:[3] The objective is to identify methods that ensure voters are not influenced or pressured into casting their votes in a particular way. This involves developing systems and protocols that protect the privacy and autonomy of voters, such as anonymous voting mechanisms and secure authentication methods. The goal is to create a voting

environment where individuals can freely express their preferences without fear of external pressures, ensuring the integrity and fairness of the election process.

4. To explore more about automating voting rules: The aim is to investigate the use of smart contracts to automatically enforce voting policies and procedures. Smart contracts, implemented through blockchain technology, can be programmed to execute predefined rules and actions based on specific conditions, eliminating the need for manual intervention of a third party. This ensures that the voting process is consistently followed, minimizing human error or manipulation and enhancing the overall efficiency and reliability of the election system. By automating voting rules, the process becomes more transparent, secure, and efficient.

5. To improve user-friendliness: The goal is to design the system in a way that is easy to use for all voters, regardless of their technical expertise.[5] This involves creating intuitive interfaces, simplifying the voting processes, and providing clear instructions at each step. The aim is to ensure that voters can easily navigate the system, cast their votes without confusion, and access any needed support, all while maintaining the security, integrity, and other features of the voting process. Enhancing user-friendliness ensures broader participation and confidence in the voting system. [24]

Chapter 02

Literature Review

2.1 Introduction

With the increasing demand for secure and transparent voting mechanisms, blockchain technology has emerged as a promising solution for e-voting. Blockchain ensures immutability, transparency, and security, addressing concerns like vote tampering, double voting, and voter anonymity. This section reviews several existing blockchain-based e-voting systems, analyzing their features, implementations, and limitations. [25]

2.2 ECC-EXONYM-eVOTING

This system integrates Elliptic Curve Cryptography (ECC) and the Exonum blockchain to ensure vote security, anonymity, and transparency. It prevents double voting and uses Idemix technology for privacy. Secure communication is maintained via the Elliptic Curve Diffie-Hellman (ECDH) protocol. The system relies on a hybrid RAFT and PBFT consensus algorithm and undergoes formal security analysis. However, its complexity, high resource demands, and lack of vote verifiability limit its adoption. [15]

2.3 A Framework to Make Voting System Transparent Using Blockchain

This system offers multiple consensus algorithms [33], with Proof of Work (PoW) as default, while supporting Proof of Stake (PoS), Ripple, and Proof of Vote. It prevents double voting using a one-time voting coin. Voter data and election results are stored immutably on the blockchain, accessible via a user dashboard. Despite its flexibility, the reliance on centralized voter databases, high computational power for PoW, and scalability issues pose significant challenges [6].

2.4 Decentralized and Automated Online Voting System

Built on ethereum and ganache [35], this system uses facial recognition for voter authentication. Votes are recorded on a distributed ledger for transparency. Smart contracts manage elections, and MongoDB stores voter and candidate data. The system ensures fault tolerance but faces challenges such as facial recognition inaccuracies, network stability issues, compromisation of the centralized database, and high database loads during peak elections. Additionally, using MetaMask for wallet management may limit accessibility for non-technical users.

2.5 E-Voting on Ethereum Blockchain

This ethereum-based system ensures vote security, transparency, and tamper resistance. It preserves voter anonymity through public-private key encryption and zero-knowledge proofs. Transactions are publicly verifiable via platforms like ropsten etherscan. However, it struggles with scalability, high ethereum gas fees [17, 31], and weak voter authentication mechanisms. Solutions like layer 2 scaling, sharding, and biometric authentication could mitigate these issues.

2.6 Iraqi Paradigm E-Voting System (Hyperledger Fabric)

This system leverages hyperledger fabric for secure, transparent, and scalable elections. It uses SHA-256 hashing for data security and allows voter verification through ID and fingerprint authentication. A certificate authority manages voter identities while election results are transparently displayed. However, the system faces challenges such as reduced efficiency with more participants, high infrastructure requirements, and lack of coercion resistance since voters can view their ballots post-election. [12]

2.7 DVTChain: A Blockchain-Based Decentralized Voting System

DVTChain uses ethereum smart contracts and a vote coin system to prevent double voting. Votes are encrypted and stored on the blockchain, ensuring verifiability and

transparency. The system operates through four phases: registration, voting setup, voting, and result announcement. Despite its security, high ethereum gas fees [31], vote-selling risks, a centralized crypto server, and energy-intensive operations pose challenges. Layer 2 scaling solutions are suggested to improve efficiency. [1]

2.8 Comparative Analysis of Existing System

Each blockchain-based e-voting system has distinct strengths and weaknesses. While some systems excel in security and transparency through cryptographic techniques and smart contracts, others focus on scalability and accessibility. However, several common limitations persist, including vote-selling risks, auditability issues, scalability constraints, high computational costs, and storage overhead.

Table 2.1 shows a comparative analysis evaluating key factors such as security, transparency, anonymity, privacy, verifiability, scalability, coercion resistance, and affordability across different systems. Additionally, Table 2.2 and Table 2.3 provide insights into why certain properties may or may not be available.

Table 2.1: Properties comparison in different implementations

Reference	SE	TR	AP	VE	SC	CR	AFF
[1]	❌	✔	✔	✔	✔	❌	❌
[6]	❌	✔	❌	✔	❌	❌	✔
[12]	❌	❌	✔	✔	✔	❌	✔
[15]	✔	❌	✔	❌	✔	✔	✔
[23]	❌	✔	✔	✔	❌	❌	❌
[24]	❌	✔	❌	❌	❌	✔	❌

Table 2.2: Reasoning for different properties in blockchain-based voting systems (part 1)

Ref	SE	TR	AP
[1]	Centralized crypto server, compromised keys affect security	Public blockchain enables voter verification	Data encrypted and hashed for privacy
[6]	Centralized database may be compromised	Results are publicly available via the dashboard	Privacy risks from a compromised database
[12]	Centralized database may be compromised	Private blockchain lacks transparency	Data hashed for privacy
[15]	Hybrid consensus, private blockchain for security	Private blockchain lacks transparency	Zero-knowledge protocol for anonymity
[23]	Lacks authentication, allowing unauthorized access	Public blockchain enables voter verification	Public and private addresses, zero-knowledge proofs for privacy
[24]	Centralized database may be compromised	Public blockchain enables voter verification	Privacy concerns about facial recognition

Table 2.3: Reasoning for different properties in blockchain-based voting systems (part 2)

Ref	VE	SC	CR	AFF
[1]	Votes verified via transaction ID after the election	Ethereum Layer 2 boosts scalability	Votes verified via transaction ID. Vote selling is possible	High energy consumption results in higher costs
[6]	Results accessible for verification	High computational power affects scalability	Vote selling risk due to user verification	No details on cost differences
[12]	Voters verify ballots after the election ends	Scalable due to private blockchain	Voters verify ballots after the election ends. Vote selling is possible	Lower cost with private blockchain
[15]	Not mentioned	Scalable due to private blockchain	Voters can't verify votes. Vote selling is not possible	Lower cost with private blockchain
[23]	Votes verified via transaction ID	Ethereum blockchain scalability issues	Votes verified via transaction ID. Vote selling is possible	Higher costs due to transaction fees
[24]	Not mentioned	Ethereum blockchain scalability issues	Voters can't verify votes. Vote selling is not possible	Higher costs due to transaction fees

SE = Security

TR = Transparency

AP = Anonymity & Privacy

VE = Verifiability

SC = Scalability

CR = Cost Reduction

AFF = Accessibility & Affordability

- Security and Privacy: Most systems emphasize encryption, smart contracts, and cryptographic techniques to secure votes and voter identities.
- Scalability Concerns: Ethereum-based systems suffer from high gas fees [32], while private blockchains have limited transaction throughput.
- Authentication Challenges: Some implementations use facial recognition and national ID verification, but OTP-based authentication remains underutilized.
- Storage Overhead: Storing encrypted votes on-chain increases costs and necessitates efficient data management strategies.

Despite significant advancements, achieving an optimal balance among security, transparency, anonymity, privacy, verifiability, scalability, coercion resistance, and affordability remains a critical challenge for blockchain-based e-voting systems [10]. Future research should focus on improving scalability, reducing cost, and enhancing authentication mechanisms to make blockchain-based voting a viable alternative for large-scale elections.

Chapter 03

Technology adapted

3.1 Introduction

To implement the proposed e-voting system, several advanced technologies have been adopted to ensure security, transparency, efficiency, and trust in the election process. These technologies include blockchain,homomorphic encryption, threshold cryptography, and a secure web interface.

3.2 Blockchain Technology

Blockchain technology is utilized to maintain a decentralized, immutable ledger for recording votes, candidate registration details, and election results. By leveraging the distributed nature of blockchain, the system ensures data integrity, transparency, and tamper-proof storage. Each transaction on the blockchain is verified by multiple nodes, preventing unauthorized modifications and ensuring trust in the election process. [22], [21]

3.3 Homomorphic Encryption

To protect voter privacy, the system employs homomorphic encryption, which allows mathematical operations to be performed on encrypted data without decryption. This ensures that votes remain confidential throughout the voting and counting phases. Only aggregated results are decrypted, preserving the anonymity of individual votes while maintaining accuracy and integrity [36].

3.4 Smart Contracts

Smart contracts are utilized to automate and enforce the rules of the election process, ensuring fairness and transparency throughout the system. They validate voter and candidate registrations, guaranteeing that only eligible participants are allowed. During the vote-counting phase, smart contracts automatically tally votes, eliminating the risk of human error or manipulation. Additionally, they publicly announce results without human intervention, enhancing trust in the election process. Solidity [34] is used for developing and deploying these smart contracts on the ethereum blockchain, leveraging its decentralized and tamper-proof nature to maintain integrity and transparency. [19]

3.5 Threshold Cryptography

Threshold cryptography is implemented to enhance security and privacy. In this system, it is used during voter authentication and vote verification processes. It allows multiple parties to jointly verify information without any single entity having full access to the data. For instance, voter authentication can be conducted by distributing cryptographic keys among multiple authorities, preventing any single point of failure and ensuring security. Similarly, threshold cryptography ensures that votes are verified collectively without exposing individual choices, maintaining both anonymity and integrity.

3.6 Off-Chain Aggregation

Off-chain aggregation is employed to efficiently handle and process encrypted votes in the electronic voting system. By performing vote aggregation outside the blockchain, the on-chain computation and storage requirements are reduced, enhancing scalability and performance. This approach maintains the integrity and confidentiality of votes while minimizing gas costs associated with blockchain transactions. Once aggregated, the encrypted results are securely submitted to the blockchain for final tallying and verification, ensuring both efficiency and transparency in the election process. [20]

3.7 Secure Web Interface

A secure web interface is designed for voter registration, candidate registration, and result announcement. It provides a user-friendly experience while ensuring data security through HTTPS encryption and multi-factor authentication. Additionally, the web interface is integrated with blockchain to display election results with full traceability, enhancing transparency and public trust.

Chapter 04

Proposed Methodology

4.1. Introduction

The proposed blockchain-based e-voting system enhances election security, transparency, and verifiability by integrating blockchain, homomorphic encryption, and threshold cryptography. It addresses traditional challenges like vote tampering and security risks while ensuring voter privacy and result integrity. Secure authentication mechanisms prevent unauthorized access [14], making the system tamper-proof, auditable, and efficient, ultimately strengthening public trust in the democratic process.

4.2 Overview of the Proposed E-Voting System Phases

We have identified five key phases for the proposed e-voting system implementation: Voter registration, candidate registration, voting, vote counting, and result announcing. Each phase is meticulously designed to address critical aspects of the election process, ensuring security, transparency, and efficiency. The Voter registration phase will focus on securely generating secret keys, authenticating and verifying voters, and ensuring only eligible participants can register and vote.[23] In the candidate registration phase, candidates will undergo a thorough verification process to confirm their eligibility, with unique identifiers assigned to each candidate for clear distinction. During the voting phase, registered voters will securely cast their votes through an encrypted system that ensures anonymity and prevents any unauthorized alterations. The Vote counting phase will automatically tally votes, using cryptographic methods to ensure accuracy and integrity, with provisions for verification and transparency. Finally, the result announcing phase will publicly disclose the election results, ensuring they are easily accessible and verifiable, reinforcing trust in the system. Together, these phases aim to deliver a robust, secure, and transparent e-voting system that instills confidence in the election process.

4.3 Voter Registration Phase

The Voter Registration Phase ensures that only eligible voters can participate in the election by implementing a secure multi-step key distribution and authentication process. This phase involves identity verification, key issuance, and secure storage to prevent unauthorized access and fraudulent voting.

4.3.1 Voter Identity Verification

The Election Commission (EC) verifies voter identities using government-issued documents and biometric authentication. Once verified, the voter details are stored in a secure database to prevent tampering and duplication.

4.3.2 Generation and Distribution of Voting Keys

Each voter is assigned a unique voting key, generated using threshold cryptography to enhance security. This key is split into two parts:

- Voter's Secret Key – Sent to the voter via a registered postal service.
- Polling Station Secret Key – Stored securely and provided to the voter upon arrival at the polling station.

The hashed voting key is stored in a secure election database to prevent tampering.

4.3.3 Issuance of Voter Secret Key

Each voter receives their unique secret key via a registered postal service. This key is essential for authentication and ensures that only the rightful voter has access. The secure delivery process prevents unauthorized individuals from obtaining the key. [9]

4.3.4 Issuance of Polling Station Secret Key

Upon arriving at the polling station, the voter is required to authenticate their identity. Once verified, election officials provide the polling station's secret key, which is unique to that voter. This ensures that each voter receives their designated key part, preventing unauthorized access and ensuring that only eligible voters can complete the key reconstruction process to cast their vote.

4.3.5 Key Reconstruction for Voting

To generate the final voting key, the voter’s secret key and the polling station's secret key are combined using threshold cryptography. This ensures that neither the voter nor the polling station officials can generate the key independently. Only the rightful voter, physically present at the polling station, can reconstruct the voting key and proceed to cast a vote.

4.3.6 Authentication and Authorization

The final voting key serves as proof of authentication, ensuring that only authorized voters can participate. This process:

- Prevents unauthorized individuals from voting on behalf of others.
- Ensures that each voter can only vote once.
- Guarantees that votes are securely cast without external manipulation.

By implementing threshold cryptography and a two-step authentication process, the system ensures that voter registration is tamper-proof, verifiable, and secure. The division of the secret key between postal delivery and polling station issuance prevents vote fraud and enhances election integrity.

4.4 Candidate Registration Phase

The candidate registration phase ensures that all candidates meet the eligibility criteria and are officially registered for the election. This process leverages blockchain technology to provide a secure, transparent, and tamper-proof registration system.

4.4.1 Candidate Application

Candidates must visit the election commission and complete the registration process following the established procedure. This involves submitting required documentation, including personal details, party affiliation, and other necessary qualifications.

4.4.2 Verification and Eligibility Check

The election commission verifies the submitted information to ensure that the candidate meets all eligibility requirements, such as age, nationality, and party affiliation. Any discrepancies or incomplete applications are addressed before proceeding.

4.4.3 Blockchain Registration

Once a candidate's eligibility is confirmed, their details are securely recorded on a private blockchain. This blockchain is initialized with a genesis block that contains the fundamental election details. The candidate’s blockchain entry includes:

- Name – Full legal name of the candidate.
- Party Affiliation – The political party they represent (if applicable).
- Symbol – The designated party or independent candidate’s symbol.
- Candidate Number – A unique identifier assigned to each candidate to ensure accurate vote allocation.

The immutable nature of blockchain ensures that candidate registration data cannot be altered or manipulated once recorded, providing transparency and security.

4.4.4 Candidate Identification and Unique Candidate ID

Each candidate is assigned a unique candidate ID once their data is registered on the blockchain. This ID is used throughout the election process to identify the candidate on ballots, vote counting, and in result announcements. The ID ensures that votes are accurately linked to the correct candidate while also preventing confusion between candidates with similar names.

4.4.5 Public Transparency and Voter Access

After candidates are registered and their information is securely stored on the blockchain, it is publicly accessible to voters through the election platform. Voters can verify candidate details, including their name, party affiliation, and symbol, in a transparent and immutable manner. Since blockchain ensures the integrity of the data, voters can trust that the information they see is authentic and has not been tampered with.

4.4.6 Final Approval

Upon successful blockchain registration and verification, the election commission gives final approval for the candidates to appear on the ballot. Once the candidate is approved and registered on the blockchain, no changes can be made unless required by election laws or regulations. This step provides a transparent and unalterable record of all candidates eligible for election.

By integrating blockchain into the candidate registration process, we hope to enhance security, ensure transparency, and create an immutable record that is accessible for

verification. This decentralized approach mitigates the risks of data manipulation and fosters trust in the election process.

4.5 Voting Phase

The Voting Phase is a critical part of the election process, ensuring voter privacy, security, and transparency. In this phase, each vote is encrypted, securely stored on IPFS [30], and made tamper-proof using blockchain technology and advanced encryption techniques. Only the IPFS hash of the encrypted vote is stored on the blockchain, ensuring both decentralization and immutability.

4.5.1 Voter Authentication and Key Reconstruction

On election day, the voter authenticates their identity using the voter's secret key and the polling station's secret key, which are combined using threshold cryptography to generate the final voting key. This ensures that only authorized voters can cast their votes and prevents fraudulent voting.

4.5.2 Ballot Casting and Homomorphic Encryption

Once the voter selects their preferred candidate, their vote is encrypted using homomorphic encryption. This advanced encryption method allows mathematical operations to be performed on the encrypted data without requiring decryption, ensuring both privacy and security throughout the voting process.

- Privacy: No entity, including the election commission or polling station officials, can view the contents of the vote.
- Integrity: The encrypted vote remains secure from any form of tampering or alteration.

- Confidentiality: The encrypted vote can only be decrypted during the counting phase to ensure the secrecy of the ballot. This combination of security measures strengthens the overall trustworthiness of the voting system.

4.5.3 Decentralized Storage of Votes on IPFS and Blockchain

Once the vote is encrypted, it is stored on IPFS (InterPlanetary File System) [30] to ensure decentralized and tamper-proof storage. The hash of the encrypted vote is recorded on the blockchain, providing an immutable record of the vote.

- Tamper-proof storage: Once recorded, the vote cannot be altered, deleted, or forged.
- Transparency and Audibility: Authorized parties can trace and audit all votes while maintaining voter anonymity.
- Security: The decentralized nature of IPFS and blockchain makes the system resistant to cyber-attacks or data corruption. This process ensures that the vote is both securely stored and verifiable without compromising voter anonymity.

4.5.4 Voter Verification and Vote Retrieval

After the voting process, voters are given the option to verify their vote. Through a user interface at the polling station, the voter can confirm that their vote has been successfully recorded on the blockchain, along with a verification receipt. [18]

- Voter Verifiability: Voters can confirm that their vote was accurately recorded.
- Privacy Protection: Since the voter cannot prove to anyone outside the polling premises which candidate they voted for, vote selling and coercion are effectively prevented. This design upholds both voter privacy and election integrity, ensuring that votes remain anonymous while allowing voters to verify participation securely. [26], [29]

By integrating threshold cryptography, homomorphic encryption, IPFS, and blockchain, this voting phase ensures that the election process is secure, transparent, verifiable, and tamper-proof.

4.6 Vote Counting Phase

The vote counting phase ensures accurate and transparent tallying of votes while preserving voter privacy and security. This process leverages homomorphic encryption to count encrypted votes without decryption, ensuring privacy throughout the process. The structured process is as follows:

4.6.1 Privacy-Preserving Vote Counting with Homomorphic Encryption

Encrypted votes stored on IPFS are retrieved, and their integrity is verified by checking the IPFS hash against the blockchain record. Homomorphic encryption is then used to compute the total votes for each candidate without decrypting individual votes. This ensures that the privacy of voters is maintained while still allowing accurate vote tallying.

- End-to-End Privacy: Votes remain encrypted during the entire counting process.
- Tamper-Resistant: The counting process is verifiable and cannot be altered.
- Scalability: Off-chain aggregation reduces computational overhead on the blockchain. This process ensures that only the final aggregated vote count is decrypted, maintaining privacy while delivering accurate election results.

4.6.2 Verifiable Vote Tallying and Decryption

Once the encrypted votes are aggregated, the final tally is decrypted using threshold cryptographic techniques. The decrypted results are then made publicly accessible, ensuring transparency in the election outcome.

- Decentralized Verification: Multiple authorities can validate the decryption process to prevent fraud.
- Public Auditability: Since vote hashes are recorded on the blockchain, independent auditors can verify the integrity of the results.
- Immutable Records: The tallying results are stored on the blockchain, ensuring they remain tamper-proof.This structured approach enhances security, ensures trust in the vote-counting process, and maintains voter anonymity.

4.7 Result Announcing Phase

The result announcing phase is the final step in the e-voting process, where the election results are made publicly available. This phase ensures transparency, accuracy, and accessibility through blockchain-based verification and a secure web interface.

4.7.1 Blockchain-Based Result Storage

Once vote counting is complete, the verified and aggregated results are stored on IPFS, with the IPFS hash recorded on the blockchain. This ensures that election results remain immutable and tamper-proof.

- Trust & Security: The results are cryptographically verifiable through blockchain records.
- Immutable Proofs: Election results cannot be altered after publication.
- Public Transparency: Voters and auditors can cross-verify results using the blockchain.

4.7.2 Secure Web Interface for Result Display

The election results are retrieved from IPFS and displayed via a secure, user-friendly web interface. This platform allows voters and stakeholders to access official election outcomes in real-time.

- Intuitive UI: Results are presented using tables, graphs, and other visual aids.
- Real-Time Access: The platform updates results as soon as they are finalized.
- Verifiable Links: Every displayed result links back to its blockchain record for verification.

By using a blockchain-backed, publicly accessible web interface, the result announcing Phase enhances trust, transparency, and confidence in the electoral process. This ensures that all results are verifiable, accurate, and secure from manipulation.

Chapter 05

Analysis and Design

This section presents the architectural design of the proposed blockchain-based e-voting system. The system is divided into multiple modules, each responsible for a specific phase of the election process. The following figures illustrate the top-level design and interactions between different components.

5.1 System Overview

The system comprises four key phases:

- Voter Registration – Ensures secure and verifiable voter enrollment.
- Candidate Registration – Registers eligible candidates securely on the blockchain.
- Voting Process – Facilitates a privacy-preserving and immutable voting mechanism.
- Counting & Result Publication – Ensures accurate and verifiable vote tallying and announcement.

Each phase is represented in the diagrams below, detailing the module interactions.

5.2 Voter Registration (Figure 5.1)

The Voter Registration Module verifies voter identities and securely assigns cryptographic voting keys. This module interacts with the election commission database to store voter records securely. There are several components related to this phase.

- Election Commission (EC): Responsible for verifying and registering voters.
- Secure Voter Database: Stores voter details (not on the blockchain).
- Threshold Cryptography Key Generation: Splits the voter's key into two parts.
- Blockchain: Stores only the hashed voter key for verification.

Process Flow:

- Voter submits registration details.
- EC verifies identity and generates a voting key pair using threshold cryptography.
- One part of the key is sent via registered mail, and the other is stored in the database and used at the polling station.
- The hashed key is stored on the blockchain for verification.

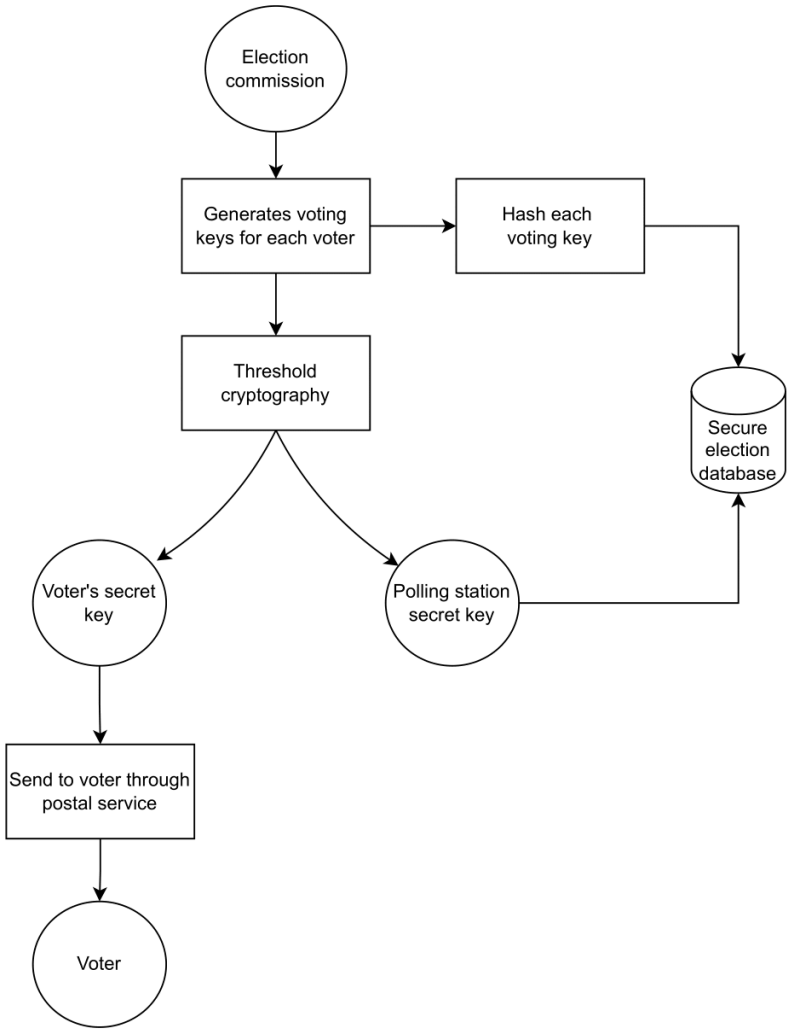

Figure 5.1: Vote Registration Process of the Proposed System

5.3 Candidate Registration (Figure 5.2)

The Candidate Registration Module ensures that only eligible candidates are registered and that their details are securely stored on the blockchain. There are several components related to this phase.

- Election Commission: Verifies and approves candidate applications.
- Candidate Database: Stores candidate details securely.
- Blockchain: Stores candidate names, party affiliations, and assigned candidate IDs in the genesis block.

Process Flow:

- Candidates submit their application with the required documents.
- EC verifies eligibility and assigns a unique candidate ID.
- Candidate details are added to the private blockchain to ensure immutability.

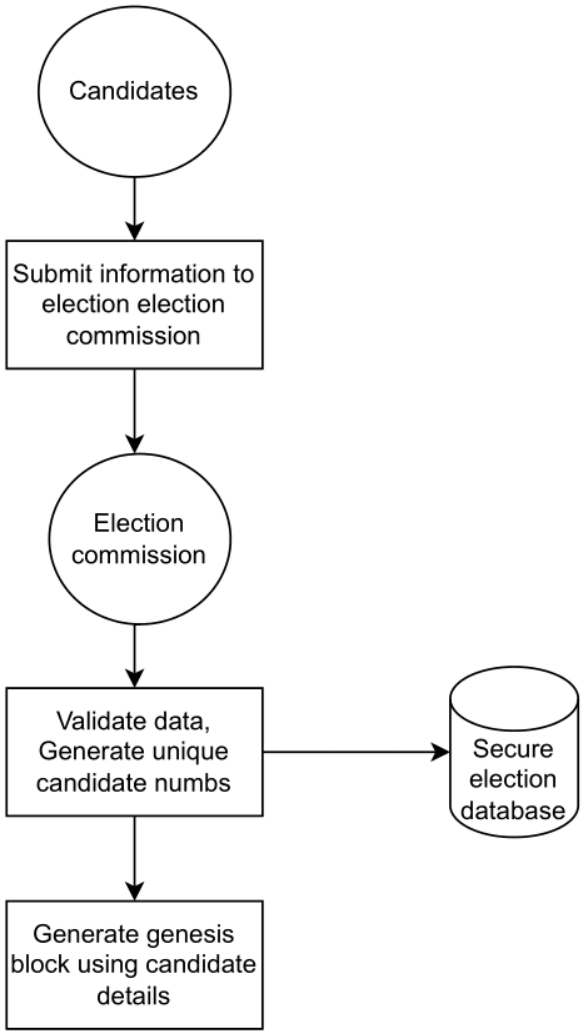

Figure 5.2: Candidate Registration Process of the Proposed System

5.4 Voting Process (Figure 5.3)

The Voting Module enables voters to cast encrypted votes securely using threshold cryptography and homomorphic encryption. Votes are stored off-chain in IPFS, while only their hashes are recorded on the blockchain. There are several components related to this phase.

- Voter Authentication: Voters must provide both key parts for authentication.
- Encrypted Ballot Casting: Votes are encrypted using homomorphic encryption.
- IPFS Storage: Encrypted votes are stored in a decentralized manner.
- Blockchain: Stores only the IPFS hash to ensure vote integrity.

Process Flow:

- Voter authenticates using both key parts.
- The voter selects a candidate.
- The vote is encrypted using homomorphic encryption and stored on IPFS.
- The IPFS hash is recorded on the blockchain.

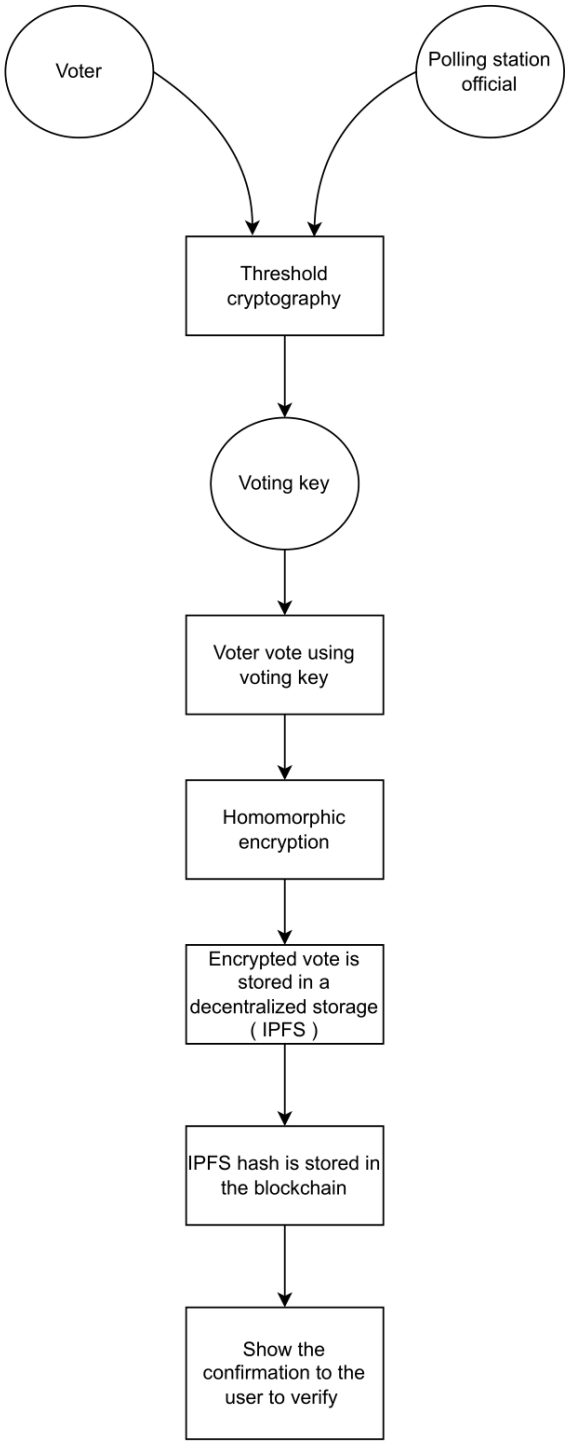

Figure 5.3: Voting Process of the Proposed System

5.5 Counting and Result Publication (Figure 5.4)

The Counting & Result Module aggregates encrypted votes off-chain using homomorphic encryption and publishes the final result on the blockchain. There are several components in this phase.

- Homomorphic Vote Aggregation: Computes results without decrypting individual votes.
- Threshold Decryption: Only the final tally is decrypted using multi-party decryption.
- Blockchain & IPFS: Stores final election results and enables public verification.
- Web Interface: Displays results in a verifiable and transparent manner.

Process Flow:

- Encrypted votes are retrieved from IPFS.
- Homomorphic encryption is used to compute vote tallies without decryption.
- The final tally is decrypted and stored on IPFS, with its hash recorded on the blockchain.
- The results are displayed via a secure web interface.

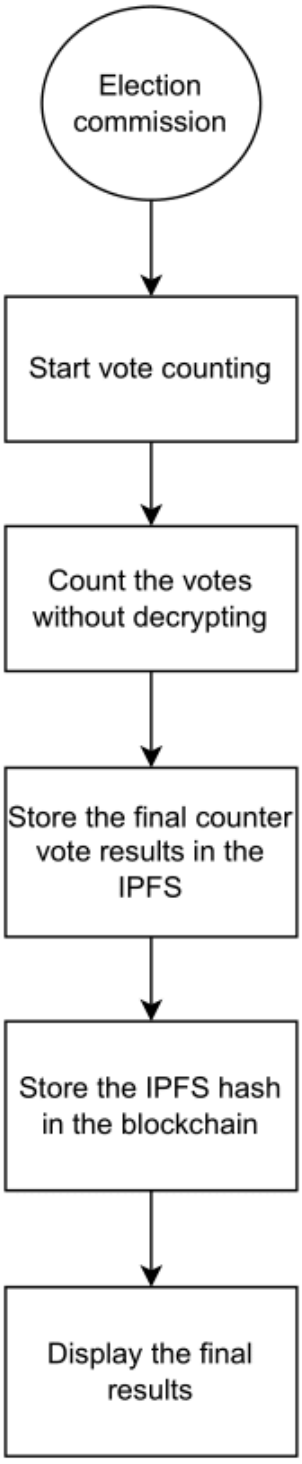

Figure 5.4: Result Counting and Publishing Process of the Proposed System

Chapter 06

Discussion

Although the system is not implemented and testing has not yet been conducted, preliminary evaluations focused on key system components, such as voter authentication, vote encryption, and blockchain-based candidate registration. Initial results indicate that the system preserves vote integrity and data immutability. Further testing is planned to assess performance and security under real-world conditions.

Planned Evaluation Approach

To ensure the system functions effectively, the following tests will be performed: Functional testing will confirm that each feature, such as vote casting and result announcement, operates as expected. Security testing will focus on resistance to vote tampering and unauthorized access. Performance testing will assess the system's response time and scalability under high voter turnout. User Acceptance Testing (UAT) will be conducted to gather feedback on usability and interface design.

This proposal presents an e-voting system with five phases: voter registration, candidate registration, voting, vote counting, and result announcing. Each phase incorporates blockchain and encryption to enhance security and transparency. Key features, such as homomorphic encryption and dual-key authentication, are designed to ensure voter privacy and trust in the system.

Conclusion

The proposed e-voting system leverages blockchain and encryption to tackle electronic voting challenges and promote election integrity. While early results are promising, thorough testing and future improvements are essential to refine the system and build public trust in its reliability and transparency.

Chapter 07

References

[1] Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University - Computer and Information Sciences, 34(9),* 6855–6871. https://doi.org/10.1016/j.jksuci.2022.06.014

[2] An, M., Fan, Q., Yu, H., An, B., Wu, N., Zhao, H., Wan, X., Li, J., Wang, R., Zhen, J., Zou, Q., & Zhao, B. (2023). Blockchain Technology Research and Application: A Literature Review and Future Trends. *Journal of Data Science and Intelligent Systems.* https://doi.org/10.47852/bonviewJDSIS32021403

[3] Dimitriou, T., & Member, S. (n.d.). Efficient, Coercion-free, and Universally Verifiable Blockchain-based Voting. http://bitcoin.org/bitcoin.pdf

[4] el Kafhali, S. (2024). Blockchain-Based Electronic Voting System: Significance and Requirements. *Mathematical Problems in Engineering, 2024.* https://doi.org/10.1155/2024/5591147

[5] Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: Evidence from eleven elections. *Government Information Quarterly, 39(4),* 101718. https://doi.org/10.1016/j.giq.2022.101718

[6] Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A Framework to Make Voting System Transparent Using Blockchain Technology. *IEEE Access, 10,* 59959–59969. https://doi.org/10.1109/ACCESS.2022.3180168

[7] Ge, Z., Loghin, D., Ooi, B. C., Ruan, P., & Wang, T. (2022). Hybrid blockchain database systems. *Proceedings of the VLDB Endowment, 15(5),* 1092–1104. https://doi.org/10.14778/3510397.3510406

[8] Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling Blockchains: A Comprehensive Survey. *IEEE Access, 8,* 125244–125262. https://doi.org/10.1109/ACCESS.2020.3007251

[9] Harn, L., Xia, Z., Hsu, C., & Liu, Y. (2020). Secret sharing with secure secret reconstruction. *Information Sciences, 519,* 1–8. https://doi.org/10.1016/j.ins.2020.01.038

[10] Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. R. (2021). The Application of the Blockchain Technology in Voting Systems. *ACM Computing Surveys, 54(3)*. https://doi.org/10.1145/3439725

[11] Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-voting system using cloud-based hybrid blockchain technology. *Journal of Safety Science and Resilience, 5(1),* 102–109. https://doi.org/10.1016/j.jnlssr.2024.01.002

[12] Jumaa, M. H., & Shakir, A. C. (2022). Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology. *Informatica, 46(6),* 87–94. https://doi.org/10.31449/inf.v46i6.4241

[13] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems, 105,* 13–26. https://doi.org/10.1016/j.future.2019.11.005

[14] Li, C., Xiao, J., Dai, X., & Jin, H. (2021). AMVchain: authority management mechanism on blockchain-based voting systems. Peer-to-Peer Networking and Applications, 14(5), 2801–2812. https://doi.org/10.1007/s12083-021-01100-x

[15] Majumder, S., Ray, S., Sadhukhan, D., Dasgupta, M., Kumar Das, A., Park, Y., Ray, S., & Park. (2022). ECC-EXONUM-eVOTING: A Novel Signature-based e-Voting Scheme using Blockchain and Zero Knowledge Property. *IEEE Open Journal of Communications*. https://doi.org/10.1109/OJCOMS.2022.1234567

[16] Marcellino, M., Wicaksana, A., & Widjaja, M. (2024). Zero-knowledge Identity Authentication for E-voting System. *Journal of Internet Services and Information Security, 14(3),* 18–31. https://doi.org/10.58346/JISIS.2024.I2.002

[17] Marchesi, L., Marchesi, M., Destefanis, G., Barabino, G., & Tigano, D. (2020). Design Patterns for Gas Optimization in Ethereum. 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), 9–15. https://doi.org/10.1109/IWBOSE50093.2020.9050163

[18] Marky, K., Kulyk, O., Renaud, K., & Volkamer, M. (2018). What did I really vote for? On the usability of verifiable e-voting schemes. *Conference on Human Factors in Computing Systems - Proceedings, 2018-April.* https://doi.org/10.1145/3173574.3173750

[19] Mccorry, P., Shahandashti, S. F., & Hao, F. (n.d.). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. http://wrap.warwick.ac.uk/112049

[20] Mühlberger, R., Bachhofner, S., Castelló Ferrer, E., di Ciccio, C., Weber, I., Wöhrer, M., & Zdun, U. (2020). Foundational Oracle Patterns: Connecting Blockchain to the Off-Chain World (pp. 35–51). https://doi.org/10.1007/978-3-030-58779-6_3

[21] Padma, D., Devayani, A., Rajeshwari Devi, K., Akhil, L., & Dinesh Karthik, R. (2025). SECURE DIGITAL VOTING SYSTEM (Vol. 21, Issue 1). www.ijerst.com

[22] Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing and Management, 58(4).* https://doi.org/10.1016/j.ipm.2021.102595

[23] Razali, M. H., Jamal, A. A., Fadzli, S. A., Zakaria, M. D., Wan Nik, W. N. S., & Hassan, H. (2025). E-Voting on Ethereum Blockchain. *Journal of Advanced Research in Applied Sciences and Engineering Technology, 50(2),* 186–194. https://doi.org/10.37934/araset.50.2.186194

[24] Sanjeeva, P., Sai Sathwik, M., Sai Prasad, G., Praneeth Reddy, G., Sajwan, V., & Ganesh, B. (2023). Decentralized and Automated Online Voting System using

Blockchain Technology. *E3S Web of Conferences, 430,* 01046. https://doi.org/10.1051/e3sconf/202343001046

[25] Shrimali, B., & Patel, H. B. (2022). Blockchain state-of-the-art: architecture, use cases, consensus, challenges and opportunities. *Journal of King Saud University - Computer and Information Sciences, 34(9),* 6793–6807. https://doi.org/10.1016/j.jksuci.2021.08.005

[26] Spadafora, C., Longo, R., & Sala, M. (2023). A COERCION-RESISTANT BLOCKCHAIN-BASED E-VOTING PROTOCOL WITH RECEIPTS. *Advances in Mathematics of Communications, 17(2),* 500–521. https://doi.org/10.3934/amc.2021005

[27] Ucbas, Y., Eleyan, A., Hammoudeh, M., & Alohaly, M. (2023). Performance and Scalability Analysis of Ethereum and Hyperledger Fabric. *IEEE Access, 11,* 67156–67167. https://doi.org/10.1109/ACCESS.2023.3291618

[28] Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J. A., & Liu, R. P. (2020). Survey: Sharding in Blockchains. *IEEE Access, 8,* 14155–14181. https://doi.org/10.1109/ACCESS.2020.2965147

[29] Ye, K., Zheng, D., Guo, R., He, J., Chen, Y., & Tao, X. (2021). A Coercion-Resistant E-Voting System Based on Blockchain Technology. *International Journal of Network Security, 23(5),* 791–806. https://doi.org/10.6633/IJNS.202109

[30] https://docs.ipfs.tech/concepts/#learn-the-basics

[31] https://www.coinbase.com/en-gb/learn/crypto-basics/what-are-gas-fees

[32] https://web3universe.today/which-blockchain-has-the-lowest-gas-fees/

[33] https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp

[34] https://docs.soliditylang.org/en/latest/

[35] https://archive.trufflesuite.com/docs/ganache/

[36] https://www.geeksforgeeks.org/homomorphic-encryption/

……

Supervisor - Prof. Manjula Sandirigama

……

Student - Kaushalya N. V. K. (E/19/193)

……

Student - Senevirathne T. N. (E/19/363)

……

Student - Silva N. H. D. U. (E/19/375

Appendixes A

Individual Contribution to the Project

Name of Student: Kaushalya N.V.K.

During the project, I focused on reviewing past research and studying existing e-voting systems. I learned about key encryption processes and advanced methods like zero-knowledge proofs (ZKPs), which verify votes without revealing the actual vote. This helped me contribute to designing a secure voter verification process for our blockchain-based voting system.

I also explored the structure of blockchain and how its decentralized nature can enhance transparency and data integrity in voting systems. Additionally, I analyzed different e-voting systems to identify common problems

Key Learnings

I deepened my understanding of encryption, blockchain, and their application in secure e-voting. ZKPs, though initially challenging, showed how privacy and verification can coexist. I also improved my documentation skills through the preparation of project reports and proposals.

Challenges and Problem Resolution

Some concepts were difficult to understand, but I tackled this by reading academic papers, using online resources, and discussing the topic with my team and our supervisor. It was also challenging to find detailed information on past e-voting systems, but expanding my research sources helped me gather the necessary data.

Although we haven't built the system yet, my contributions to the literature review and proposal provided a strong foundation for future development. This project helped me enhance my research and analytical skills.

Name of student: Senevirathne T. N. (E/19/363)

My main contributions to the blockchain-based e-voting system project included conducting research, reviewing literature, and drafting key documents. I explored various blockchain-based voting systems, their advantages, and security mechanisms. Additionally, I wrote the literature review and project proposal, outlining objectives, methodology, and security measures.

Contributions

- Researched blockchain-based voting systems, focusing on security, transparency, and cryptographic techniques like zero-knowledge proofs and homomorphic encryption.
- Analyzed different blockchain architectures and their suitability for secure voting.
- Wrote the literature review and project proposal, defining problems, methodologies, and expected outcomes.

What I Learned

- Gained in-depth knowledge of blockchain technology, smart contracts, and cryptographic techniques used in voting systems.
- Improved technical writing and analytical skills through research and documentation.

Challenges and Solutions

- Understanding complex blockchain concepts – Simplified through structured research and online courses.
- Identifying secure implementation models – Categorized existing solutions to compare feasibility.
- Analyzing security vulnerabilities – Consulted multiple sources to understand risks and mitigation strategies.

Name of student: Silva N. H. D. U. (E/19/375)

My main contributions to the project were conducting research, writing the literature review, and preparing the project proposal. I studied various research papers to understand traditional voting systems, their limitations, and how blockchain can enhance security and transparency.

I explored different blockchain types, consensus mechanisms, smart contracts, and cryptographic techniques like zero-knowledge proofs and threshold cryptography. Additionally, I analyzed existing blockchain-based e-voting implementations, identifying their strengths and weaknesses.

Writing the project proposal involved defining key system components, including voter registration, candidate registration, secure voting, and transparent result publication. I also contributed to the initial system design by creating high-level diagrams.

Challenges included filtering relevant information from vast research material and understanding complex cryptographic methods, which I addressed through structured analysis and extensive reading.

Through this process, I gained valuable insights into blockchain security, decentralized voting, and research methodologies, strengthening both my technical and analytical skills.