
Securing E-Voting in Bangladesh : A Blockchain Based System

By

Nusrat Jahan
012222003

Submitted in partial fulfilment of the requirements
of the degree of Master of Science in Computer Science and Engineering

January 24, 2026



Department of Computer Science and Engineering
United International University

Approval Certificate

This project titled ‘**Securing E-Voting in Bangladesh : A Blockchain Based System**’ submitted by ‘**Nusrat Jahan**’, Student ID: ‘**012222003**’, has been accepted as **Satisfactory** in fulfillment of the requirement for the degree of Master of Science in Computer Science and Engineering on 24th January, 2026.

Board of Examiners

1.

Supervisor

Mr. Mohammad Mamun Elahi
Assistant Professor
Dept. of Computer Science and Engineering
United International University
Dhaka Bangladesh

2.

Examiner

Dr. Mohammad Shahriar Rahman
Professor
Dept. of Computer Science and Engineering
United International University
Dhaka Bangladesh

3.

Ex-Officio

Prof. Khondaker A. Mamun, PhD.
Professor
Dept. of Computer Science and Engineering
MSCSE Program & Director
Director IRIIC
United International University
Dhaka Bangladesh

Declaration

This is to certify that the work entitled ‘**Securing E-Voting in Bangladesh : A Blockchain Based System**’ is the outcome of the project carried out by me under the supervision of ‘**Mr. Mohammad Mamun Elahi, Assistant Professor**’

Nusrat Jahan
MSCSE Program
Student ID: 012222003
Dept. of Computer Science and Engineering
United International University
Dhaka, Bangladesh

In my capacity as supervisor of the candidate’s project, I certify that the above statements are true to the best of my knowledge.

Mr. Mohammad Mamun Elahi
Assistant Professor
Dept. of Computer Science and Engineering
United International University
Dhaka Bangladesh

Abstract

The electronic voting process brings a technological advancement to ballot casting. It blends tradition with technology. The system presents digital capabilities which guarantee both improved security and efficiency in operations. Previous e-voting implementations frequently experience problems at present. Democratic systems receive criticism because of their virtual weaknesses. The system permits security breaches while displaying minimal transparency while weakening vote privacy. This research investigates the development of blockchain-enabled e-voting (BEV) as a solution for resolving the existing problems within voting systems. The project development targets improvements in election security together with privacy systems and enhanced reliability features. Our system deploys blockchain essential attributes which include decentralization, transparency and immutability. Research determines how BEV functions as an election technology in Bangladesh. The report takes a confident stance to compare Bangladesh's digital voting system with the digital voting pioneers of Estonia and Switzerland. The research proves blockchain uses security protocols to prevent Vote alteration and duplication events. Blockchain operates as an effective system to prevent accidental modifications in addition to unauthorized alterations. The system helps authorize voter identification. At the same time we fully recognize the critical need for actual field tests regarding this matter. Bangladesh needs to address its infrastructure challenges along with raising standards of voter privacy in its one-of-a-kind geographic setting. The research establishes that blockchain technology establishes active and transparent digital election procedures which provide security. The importance of future examination becomes crucial to solve both technical problems and regulatory requirements with blockchain technology. These findings are meant to serve as practical guidance for Bangladeshi policy makers together with other stakeholders. The researchers strive to enhance blockchain election functions and develop secure trusted electronic voting infrastructure.

Acknowledgements

All the praises and thanks are to Allah, the most gracious and the ever merciful. HE has given me the strength, courage, and patience to carry out this work.

Then, this project represents a great deal of time and effort not only on my part but also on the part of my supervisor, Assistant Prof. Mr. Mohammad Mamun Elahi.

I am also thankful to my project committee members for providing insightful and constructive comments to improve the quality of this project.

Then thanks to family and friends for their continuous support, understanding, and motivation during the completion of this thesis.

Table of Contents

Table of Contents	vii
List of Figures	viii
List of Tables	ix
1 Introduction	1
2 Blockchain	3
2.1 Blockchain	3
2.1.1 Technical Insights into Blockchain Applications	3
2.2 Structure of a Block	4
2.2.1 NIST Standards and the Role of SHA-256	4
2.3 Linking Blocks Together	5
2.4 Adding New Blocks	5
3 Background and Literature Review	6
3.1 Electronic Voting Systems: Evolution and Challenges	7
3.1.1 Estonian I-Voting System	7
3.1.2 Norwegian I-Voting System	7
3.1.3 New South Wales iVote System	7
3.1.4 Washington D.C. Digital Vote-by-Mail Service	7
3.1.5 Verification Flaws and Security Failures	7
3.1.6 Anonymous Voting and Blind Signatures	8
3.2 Blockchain-Based E-Voting Systems: Opportunities and Cases	8
3.2.1 Security and Decentralization	8
3.2.2 Privacy and Transparency	8
3.2.3 Post-Quantum Cryptography	8
3.2.4 Real-World Applications	8
3.2.5 Cryptographic Incorruptibility	9
3.2.6 Voter Anonymity and Auditability	9
3.3 Comparative Analysis and Empirical Outcomes	9
3.4 Gap Analysis and Future Research Directions	9

4	Project Overview	11
4.1	Scope of Work	11
4.2	Requirements	11
4.2.1	Tools and Technologies Used	11
4.2.2	Development Environment Setup	12
4.2.3	Platform Dependencies	12
4.3	Step-by-Step Setup Guide	12
4.3.1	Install Prerequisites	12
4.3.2	Set Up a Virtual Environment	12
4.3.3	Install Dependencies	12
4.3.4	Run the Application	13
4.4	Database Setup	13
4.4.1	Using SQLite (Default)	13
4.4.2	Using MySQL or PostgreSQL	13
5	API Testing	15
5.1	Identifying API Endpoints	15
5.2	Testing APIs with cURL	15
5.3	Testing with Postman	15
5.4	Automating API Testing Using Python	16
5.5	Troubleshooting and Debugging	17
5.6	Summary	17
6	Methodology	18
6.1	System Requirements	18
6.1.1	Authentication	19
6.1.2	Anonymity	19
6.1.3	Accuracy	19
6.1.4	Verifiability	19
6.2	Blockchain Implementation	20
6.2.1	Blockchain Structure	20
6.2.2	Voting Process	20
6.2.3	Protest Vote	20
6.2.4	Decentralization	20
6.3	Voting Process Steps	21
6.3.1	Requesting to Vote	21
6.3.2	Casting a Vote	21
6.3.3	Vote Encryption	21
6.3.4	Including the Vote in the Blockchain	21
6.4	Conflict Resolution with Blockchain	22
6.4.1	Sybil Attacks and Blockchain Mitigation	22

6.4.2	Longest Chain Principle	22
6.5	Information Security and Cryptography	22
6.6	Experimental Design and Validation	23
6.6.1	Experimental Components	23
6.6.2	Quantum-Resistant Security	23
6.7	Algorithmic Workflow and Flowcharts	23
6.7.1	Pseudo Code	24
6.8	Summary	25
7	Prototype Testing	27
8	Limitation & Challenges	31
8.0.1	Limitations	31
8.0.2	Challenges	31
9	Conclusion	34
	References	35

List of Figures

2.1	Figure 1: SHA-256 Hash Function: Input-to-Hash Process	4
2.2	Figure 2: Blockchain Voting Process Using SHA-256 Hash Function	5
6.1	Key Features of a Blockchain-Based E-Voting System	18
6.2	Requirements for a Blockchain-Based E-Voting System	19
6.3	Vote Chaining for Multiple Candidates in a Blockchain System	20
6.4	Blockchain-Based E-Voting Workflow: Voter to Blockchain Integration	21
6.5	Forked Blockchain Representation: Main Chain and Diverging Blocks	22
6.6	Conflict Resolution in Blockchain: Longest Chain Rule and Orphan Blocks	23
6.7	Pilot Design for Blockchain Voting Systems	24
6.8	Blockchain Voting Workflow	26
7.1	Vote Selection	27
7.2	Blockchain Mined	28
7.3	Tracking Results	28
7.4	Longest Chain with Hash and data	29
7.5	Results Summary	29

List of Tables

3.1	Comparison of Existing Electronic Voting Systems and the Proposed Blockchain-Based Voting System	10
5.1	API Endpoints and Their Purposes	15
5.2	Common Issues and Solutions	17

Chapter 1

Introduction

Contemporary advancement of the electronic voting (e-voting) has been identified as an effective way of enhancing the voting procedures while observing the best standards of efficiency and accommodation for voters. Nonetheless, similar to any other Internet applications, e-voting systems still pose challenges in security, transparency and most importantly confidence. The issues of vote modifying and vote hacking, impostures, votes buying and selling and even losing of the votes reveal more doubts about the efficiency of these systems in recording true voters' decisions. Further, the anonymity of voters is not normally well safeguarded and this could result in a violation of the voter's rights to privacy. The existing e-voting systems have some limitations, and so, researchers have looked for blockchain technology to reduce these risks and increase the accuracy of online voting.

Blockchain is an emerging technology that creates a distributed and secure database in which the recording of the transaction is preserved in a transparent way that attracts many applications, including voting. With the help of its cryptographic characteristics and decentralized structure, blockchain corrects the significant weakness of e-voting. For instance, the consensus algorithms and cryptography of blockchain eliminate vote rigging and unauthorized interference, once a vote has been placed, it is safe and cannot be changed. These properties one on one combat normal vices in a voting process including vote buying, voter fraud, and vote doubling. Therefore, there is a possibility of establishing a voting system whose individual votes are already verified, anonymous, and stored in a decentralized way thereby minimizing election fraud. There is an increasing number of works focusing on the opportunities Blockchain opens for the e-voting systems proposing a new framework of security, transparency and voters anonymity. Madise & Martens [1] continue this thread by propounding a blockchain-based e-voting system that reduces the incidences of fraud and manipulation due to cryptographic processes being incorruptible. Their work augments the understanding of how adopted characteristics of blockchain can improve the veracity of electronic voting systems. In the same way, Yedhukrishnan [2] provided a survey on blockchain-based e-voting which addressed the technological and social point of view of this system. In their paper, they also cover the relative advantages of

the system, which cannot be discussed in isolation from its weaknesses: the issues with scalability and the overall difficulty of applying blockchain. Kolte[3] review the state of e-voting decentralized applications and cross-platform comparison, and potential avenues of development for blockchain voting systems. All this research taken together paints a picture of what blockchain is capable of while pointing to its shortcomings and the ways it can be developed further.

The application of Distributed Permission Ledger Technology (DPLT) on Solana blockchain with e-voting technology led to the successful digital voting of more than 1,200 ballots without incidents of fraud or tampering in Morocco according to [4]Blockchain-based electronic voting systems: A case study in morocco. The International Journal of Blockchain Applications published a review by Johari[5] which demonstrated that European small-scale elections using blockchain technology delivered an 87% satisfaction rate from voters because of improved transparency and enhanced security. The research shows blockchain has the power to transform voting systems into secure operation with increased efficiency. Following the research done by other scholars, this study employs a comparative analysis of different blockchain based implementations of e-voting with specific emphasis on Estonia and Switzerland. Both countries have led efforts to introduce digital voting, so they are well suited to the exploration of the impact of blockchain technology on actual electoral processes. To contribute to the understanding of blockchain's future application in election systems, this paper reviews the advantages and limitations of e-voting schemes and compares them with the specified blockchain implementations. In addition to the analysis of blockchain solutions in e-voting, this work is also aimed at helping policymakers and technologists better understand which issues one needs to expect when implementing blockchain technology to democratic procedures. Finally, this study aims at advancing the age-old goal of developing a secure, trustworthy, and easily scalable e-voting system in response to the challenges that democracies of the present world face.

Chapter 2

Blockchain

2.1 Blockchain

Blockchain was invented by an anonymous figure, Satoshi Nakamoto[6], as part of a methodology for a digital currency that could be transferred electronically between parties with assurance of authenticity and without third-party endorsement. This system was introduced in 2009 through Bitcoin, where cryptographic techniques were employed to enable a decentralized and secure method of exchanging digital currency online.

Blockchain can be described as a structured sequence of data blocks, where each block contains multiple transactions. Each block is cryptographically linked to the previous block, forming a continuous chain known as a blockchain. The chain begins with the *genesis block*, which serves as the first block in the system. Every newly created block is appended sequentially to the preceding block, preserving data integrity and chronological order.

2.1.1 Technical Insights into Blockchain Applications

According to Raval[7], blockchain technology has undergone significant advancements since its inception and has become the foundation for many decentralized applications. Raval highlights the importance of cryptographic hashing techniques to ensure data integrity and the use of decentralized consensus mechanisms to reduce reliance on central authorities.

A critical component of blockchain systems is the implementation of smart contracts. These are self-executing contracts where the terms and conditions are enforced algorithmically. Smart contracts enable secure, transparent, and trust-less transactions, which are essential for applications such as Decentralized Finance (DeFi), supply chain management, and electronic voting systems. Raval[7] further explains that blockchain technology is adaptable and applicable beyond digital currency, extending into various real-world domains.

This technical perspective emphasizes both the robustness and flexibility of blockchain systems in managing large volumes of transactions. Such understanding is essential for

identifying real-life problems that can be effectively addressed through blockchain technology, particularly from a security and system design standpoint.

2.2 Structure of a Block

Each block in a blockchain consists of several key components:

- **Block Size:** Represents the total size of the block, which may contain one or more transactions.
- **Block Header:** Contains metadata including a cryptographic hash generated using the Secure Hash Algorithm (SHA-256). This hash uniquely identifies the block and ensures its integrity.

2.2.1 NIST Standards and the Role of SHA-256

The SHA-256 cryptographic hash algorithm, standardized by the National Institute of Standards and Technology (NIST) in 2012[8], plays a crucial role in blockchain security. This algorithm produces a fixed-length 256-bit hash for any input data, making it computationally infeasible to derive the original input or generate another input that produces the same hash.

NIST (2012)[8] provides detailed guidelines on SHA-256, emphasizing its resistance to collision and pre-image attacks. Due to these properties, SHA-256 is widely used in blockchain systems to secure transaction data and block headers, ensuring immutability and trustworthiness. NIST's cryptographic standards remain fundamental as blockchain technology continues to evolve.

- **Transaction Counter:** Tracks the number of transactions included within a block.
- **Transactions:** Store the actual transaction data. Each block header is encrypted using SHA-256, a one-way cryptographic function developed by the National Security Agency (NSA), producing a fixed-size output that cannot feasibly be reversed.

Figure 2.1 illustrates the SHA-256 input-to-hash process.

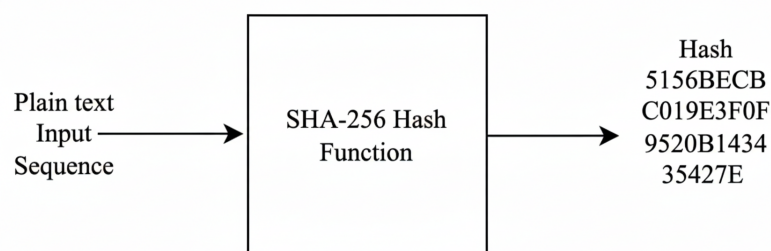


Figure 2.1: Figure 1: SHA-256 Hash Function: Input-to-Hash Process

2.3 Linking Blocks Together

A defining characteristic of blockchain technology is the cryptographic linkage between blocks. Each block header contains the hash of the previous block, creating an immutable chain. Any modification to a single block would invalidate all subsequent blocks, as their stored hash references would no longer match.

2.4 Adding New Blocks

When a new block is created, it is validated and appended to the existing blockchain. This process occurs continuously, with each new block referencing the hash of the previous one. In an electronic voting system, for example, votes are grouped into a block, encrypted using SHA-256, and added to the blockchain. Each new vote strengthens the system's decentralization, confidentiality, and immutability.

Figure 2.2 illustrates the blockchain-based voting process using SHA-256.

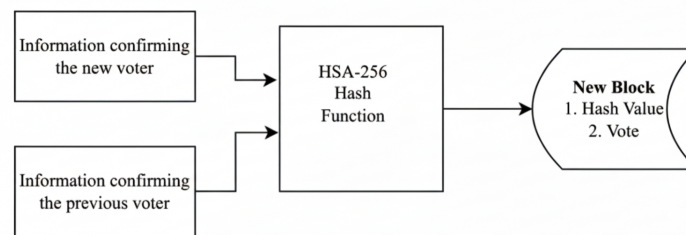


Figure 2.2: Figure 2: Blockchain Voting Process Using SHA-256 Hash Function

This decentralized architecture enhances security by eliminating single points of failure. Any attempt to alter stored data would disrupt the cryptographic linkage between blocks, making blockchain a highly suitable solution for security-sensitive applications such as electronic voting.

Chapter 3

Background and Literature Review

Electronic voting (e-voting) has emerged as a potential alternative to traditional paper-based voting systems, offering advantages such as convenience, reduced operational costs, and time efficiency. Despite these benefits, e-voting systems face significant security challenges that hinder their widespread adoption. Major concerns include threats to voter identity, vote manipulation, vulnerability to cyber-attacks, and lack of transparency. These challenges have motivated researchers and practitioners to explore blockchain technology as a means to enhance the security and reliability of e-voting systems.

Blockchain is a shared, distributed, and publicly verifiable transaction ledger operating over the internet. Its inherent characteristics—decentralization, cryptographic security, and immutable audit trails—directly address many of the limitations associated with conventional e-voting systems. Unlike centralized architectures, blockchain eliminates single points of control, thereby reducing the risk of manipulation. Furthermore, cryptographic mechanisms ensure vote authenticity while preserving voter anonymity, making it impossible to alter or delete votes once recorded.

Summary

Blockchain technology presents significant potential for improving electronic voting systems by addressing core issues related to security, transparency, and voter privacy. Although blockchain remains an evolving and experimental technology, its capabilities in reshaping digital voting infrastructures indicate a strong possibility of transforming electoral processes. Continued research and real-world experimentation are essential to overcome existing challenges, with a focus on developing blockchain-based voting systems that are both legally compliant and technologically robust for future elections worldwide.

3.1 Electronic Voting Systems: Evolution and Challenges

The evolution of electronic voting systems can be traced back to the 1980s, when David Chaum introduced the concept of anonymous voting through the Blind Signature Theorem. This foundational work aimed to separate voter identity from the actual vote, laying the groundwork for modern electronic voting mechanisms. Subsequent developments led to systems such as Direct Recording Electronic (DRE) voting machines and Internet-based voting systems.

Various countries have implemented e-voting systems with differing approaches:

3.1.1 Estonian I-Voting System

Estonia became the first country to conduct nationwide internet voting in 2005 using a national electronic identity (e-ID) system [1]. The system employed SHA-1 and SHA-2 cryptographic algorithms along with a 2048-bit PIN to ensure vote security and allowed voters to cast multiple votes, counting only the latest submission. Despite its innovation, concerns regarding transparency and the use of proprietary code have been raised.

3.1.2 Norwegian I-Voting System

Norway introduced internet voting during its municipal elections in 2011. However, the system was discontinued in 2014 due to security concerns, including potential vote leakage and cyber vulnerabilities [9].

3.1.3 New South Wales iVote System

The New South Wales iVote system was deployed during the 2015 state elections, enabling over 280,000 voters to participate electronically. While the system enhanced accessibility, issues related to closed-source components and verification weaknesses raised transparency concerns [10].

3.1.4 Washington D.C. Digital Vote-by-Mail Service

In 2010, Washington D.C. piloted an online vote-by-mail system. The project was ultimately abandoned after security testing revealed critical vulnerabilities, highlighting inherent risks in early e-voting systems [11].

These cases illustrate persistent challenges related to secrecy, centralization, and susceptibility to cyber-attacks. As a result, researchers have increasingly turned to blockchain technology as a potential enhancement to traditional e-voting architectures.

3.1.5 Verification Flaws and Security Failures

Verification flaws in the New South Wales iVote system were identified during live elections, exposing significant security weaknesses [10]. Similarly, the Washington D.C. Digital Vote-

by-Mail system was found vulnerable to cyber-attacks, leading to its termination [11]. These failures emphasize the need for more resilient voting technologies.

3.1.6 Anonymous Voting and Blind Signatures

The concept of anonymous electronic voting based on the Blind Signature Theorem was first introduced by Chaum in 1983. This approach became the cornerstone of many modern e-voting systems by ensuring voter privacy while maintaining vote verifiability [12].

3.2 Blockchain-Based E-Voting Systems: Opportunities and Cases

The limitations of conventional e-voting systems have led to the exploration of blockchain-based alternatives. Blockchain offers decentralization, resistance to tampering, and verifiable yet anonymous voting mechanisms. Several studies highlight its potential:

3.2.1 Security and Decentralization

Gupta [13] proposed a blockchain-based e-voting model that eliminates centralized control and enhances transparency. Their findings suggest that encrypted votes recorded on a blockchain cannot be altered, while still allowing voters to independently verify their participation.

3.2.2 Privacy and Transparency

Kolte [3] demonstrated that blockchain-based voting systems can achieve both voter anonymity and public auditability. Their work shows that election transactions can be transparently verified without revealing voter identities.

3.2.3 Post-Quantum Cryptography

To address future threats posed by quantum computing, Laia and Barmawi [14] explored the integration of post-quantum cryptography into blockchain-based e-voting systems. Their model strengthens the cryptographic foundation of blockchain against emerging computational threats.

3.2.4 Real-World Applications

The paper "Strengthening the Authentication Mechanism of Blockchain-Based E-Voting System Using Post-Quantum Cryptography" says [14] proposed a blockchain-based liquid democracy voting system implemented on the Ethereum platform. Their work demonstrates the feasibility and adaptability of blockchain for practical electoral applications.

3.2.5 Cryptographic Incorruptibility

Johari[5] emphasized the role of cryptographic incorruptibility in blockchain-based voting systems. By employing SHA-256 hashing, their approach ensures vote immutability, addressing a major weakness of traditional e-voting systems.

3.2.6 Voter Anonymity and Auditability

Yedhukrishnan[2] highlighted blockchain’s ability to ensure voter anonymity while enabling verifiable transactions. Their approach supports secure auditing through blockchain transaction logs without compromising voter identity.

3.3 Comparative Analysis and Empirical Outcomes

Estonia[15] is often cited as a technologically prepared nation for blockchain-based voting due to its advanced digital infrastructure, despite not directly using blockchain in its voting system. Similarly, blockchain-based voting trials in Switzerland[16] have demonstrated improved data integrity and increased public trust by securely managing voting data on distributed ledgers.

3.4 Gap Analysis and Future Research Directions

Despite promising developments, several challenges remain before blockchain-based e-voting systems can be widely adopted. Key unresolved issues include scalability, regulatory compliance, and user accessibility. Comparative analysis indicates the need for further research on blockchain’s resilience against advanced cyber threats, its ability to scale for national elections, and public acceptance. Future research should focus on best practices, hybrid public-private blockchain models for enhanced privacy, and the broader societal impact of blockchain-based voting systems.

Table 3.1: Comparison of Existing Electronic Voting Systems and the Proposed Blockchain-Based Voting System

Feature	Estonian Voting [1]	Norwegian Voting [9]	New South Wales iVote [10]	Washington D.C. Digital Vote-by-Mail [11]	Proposed Blockchain System
Authentication	National e-ID + PIN	National ID	ID + PIN + Receipt	Address + Pre-registered Credentials	Pre-registered voter list, hashed ID
Anonymity	Partial (votes tied to IDs, latest vote counted)	Limited (risk of breaches)	Partial (identifiable receipt)	Poor (linked to voter data)	Fully anonymous via SHA-256 encryption
Transparency	Limited (proprietary code)	Limited (not open-source)	Limited (closed components)	Minimal (security vulnerabilities exposed)	Public, auditable blockchain ledger
Decentralization	Centralized	Centralized	Centralized	Centralized	Fully decentralized
Cryptographic Security	SHA-1 / SHA-2 encryption	Standard encryption	Standard encryption	Minimal	SHA-256 + post-quantum cryptography
Scalability	National elections	Local elections	Regional elections	Local trials	Potential global scalability
Conflict Resolution	Not applicable	Not applicable	Not applicable	Not applicable	Longest Chain Rule
Accessibility	High	Moderate	High	Low (discontinued)	High with mobile and web interfaces
User Verifiability	Limited	Minimal	Partial (receipt)	None	Full, via blockchain transaction logs
Resistance to Cyber-Attacks	Moderate	Poor	Moderate	Poor	High (blockchain and quantum-resistant)
Regulatory Compliance	Established	Moderate	Moderate	Minimal	Needs further research

Chapter 4

Project Overview

The Blockchain E-Voting System is a secure and decentralized voting platform designed to ensure transparency and immutability through blockchain technology. This chapter provides a comprehensive guide for setting up the development environment, installing dependencies, configuring the database, and testing application programming interfaces (APIs).

4.1 Scope of Work

The primary objective of this project is to develop a secure, verifiable, and transparent electronic voting system based on blockchain technology. The system aims to address the limitations of conventional e-voting platforms by incorporating strong cryptographic mechanisms, decentralization of voting infrastructure, and transparent data handling. Through these features, the system seeks to enhance voter privacy, reduce opportunities for fraud, and build trust in the electoral process.

4.2 Requirements

4.2.1 Tools and Technologies Used

- **Programming Language:** Python 3.7+
- **Web Framework:** Flask (for API development)
- **Blockchain Mechanism:** Custom Proof-of-Work implementation
- **Database:** SQLite (default), PostgreSQL/MySQL (optional)
- **Testing Tools:** Postman, cURL, Python `requests` library
- **Version Control:** Git (optional)

4.2.2 Development Environment Setup

- **Operating System:** Windows / Linux / macOS
- **Virtual Environment:** Python venv
- **Server:** Flask Development Server
- **Package Manager:** pip

4.2.3 Platform Dependencies

- Python 3.7 or later installed
- Flask installed (`pip install flask`)
- Database (SQLite, MySQL, or PostgreSQL)
- Postman (for API testing)
- Git (optional, for version control)

4.3 Step-by-Step Setup Guide

4.3.1 Install Prerequisites

Ensure Python and Git are installed:

```
python --version
pip --version
git --version
```

4.3.2 Set Up a Virtual Environment

Create a virtual environment:

```
python -m venv evoting_env
```

Activate the environment:

- **Windows:** `evoting_env\Scripts\activate`
- **Linux/macOS:** `source evoting_env/bin/activate`

4.3.3 Install Dependencies

Navigate to the project directory and install required packages:

```
cd /path/to/Evoting_System
pip install -r requirements.txt
```

4.3.4 Run the Application

```
python app.py
```

Expected output:

Running on `http://127.0.0.1:5000/`

4.4 Database Setup

4.4.1 Using SQLite (Default)

SQLite requires no additional configuration. If the database file does not exist, create it:

```
python
from app import db
db.create_all()
exit()
```

4.4.2 Using MySQL or PostgreSQL

Install Database

- **MySQL:** Download from official website
- **PostgreSQL:** Download from official website

Create Database

For MySQL:

```
mysql -u root -p
CREATE DATABASE evoting_db;
```

For PostgreSQL:

```
psql -U postgres
CREATE DATABASE evoting_db;
```

Configure the Project

Update `config.py`:

MySQL:

```
SQLALCHEMY_DATABASE_URI = 'mysql+pymysql://username:password@localhost/evoting_db'
```

PostgreSQL:

```
SQLALCHEMY_DATABASE_URI = 'postgresql://username:password@localhost/evoting_db'
```

Apply Migrations

```
flask db upgrade
```

Alternatively, create tables manually:

```
python
from app import db
db.create_all()
exit()
```

Chapter 5

API Testing

5.1 Identifying API Endpoints

Table 5.1: API Endpoints and Their Purposes

Endpoint	Method	Purpose
/register	POST	Register a voter
/vote	POST	Cast a vote
/results	GET	View election results
/mine	GET	Perform mining for blockchain
/chain	GET	View the blockchain

5.2 Testing APIs with cURL

Retrieve blockchain data:

```
curl -X GET http://127.0.0.1:5000/chain
```

Cast a vote:

```
curl -X POST http://127.0.0.1:5000/vote \  
-H "Content-Type: application/json" \  
-d '{"voter_id":"123","candidate":"Alice"}'
```

Mine a new block:

```
curl -X GET http://127.0.0.1:5000/mine
```

5.3 Testing with Postman

1. Open Postman.

2. Select request type (POST).
3. Enter URL: `http://127.0.0.1:5000/vote`
4. Go to Body → Raw → JSON.
5. Enter the following data:

```
{  
  "voter_id": "123",  
  "candidate": "Alice"  
}
```

Click **Send** and verify the response.

5.4 Automating API Testing Using Python

```
import requests  
  
BASE_URL = "http://127.0.0.1:5000"  
  
def get_chain():  
    response = requests.get(f"{BASE_URL}/chain")  
    print("\nBlockchain Data:", response.json())  
  
def cast_vote(voter_id, candidate):  
    data = {"voter_id": voter_id, "candidate": candidate}  
    response = requests.post(f"{BASE_URL}/vote", json=data)  
    print("\nVote Response:", response.json())  
  
def mine_block():  
    response = requests.get(f"{BASE_URL}/mine")  
    print("\nMining Response:", response.json())  
  
def main():  
    print("Starting API Tests...")  
    get_chain()  
    cast_vote("123", "Alice")  
    mine_block()  
    get_chain()  
  
if __name__ == "__main__":  
    main()
```

Run the script:

```
python api_test_evoting.py
```

5.5 Troubleshooting and Debugging

Table 5.2: Common Issues and Solutions

Issue	Solution
Connection Refused	Ensure <code>python app.py</code> is running
500 Internal Server Error	Check application logs for missing data
No Response	Verify API endpoint definitions

5.6 Summary

The Blockchain E-Voting System has been successfully configured and tested. The system utilizes Flask for API development, relational databases for data storage, and a blockchain mechanism to secure voting records. API functionality has been validated using cURL, Postman, and automated Python scripts, ensuring robustness and reliability of the proposed system.

Chapter 6

Methodology

This chapter presents the methodology adopted to design and implement a blockchain-based electronic voting (e-voting) system. The proposed approach aims to overcome the limitations of conventional electronic voting systems by enhancing security, anonymity, accuracy, and verifiability through blockchain characteristics such as decentralization, transparency, cryptographic security, and immutability.

The methodology follows a step-by-step framework that explains the system requirements, blockchain implementation, voting workflow, conflict resolution mechanisms, experimental validation, and algorithmic design. The initial stage of the methodology is illustrated in Figure 6.1.

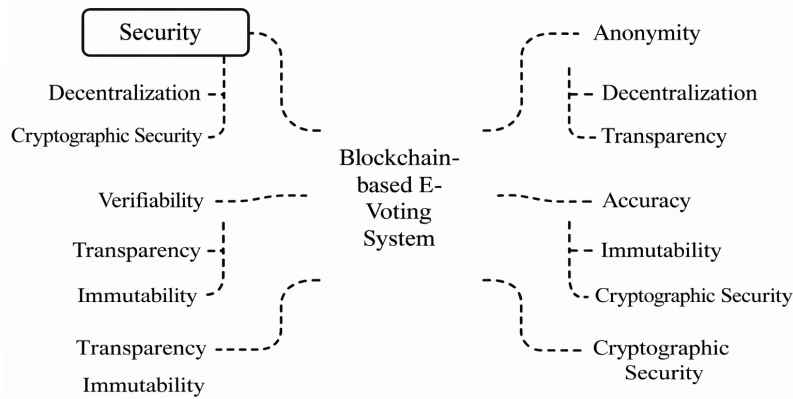


Figure 6.1: Key Features of a Blockchain-Based E-Voting System

6.1 System Requirements

To ensure a secure, anonymous, accurate, and verifiable blockchain-based e-voting system, the following requirements are incorporated into the system design:

6.1.1 Authentication

Only pre-registered voters are permitted to cast votes. Voter registration occurs outside the system due to legal and procedural constraints related to credential verification. During the voting process, the system cross-checks voter credentials against a verified database to ensure eligibility and prevent multiple voting attempts by the same individual.

6.1.2 Anonymity

The system preserves voter anonymity by ensuring that no direct link exists between a voter and their ballot. This principle is fundamental to maintaining voter trust and ensuring freedom of choice during elections.

6.1.3 Accuracy

All votes are recorded as immutable digital records that cannot be altered or deleted. The system accurately counts votes and enables traceability in the event of any attempt to manipulate stored voting data.

6.1.4 Verifiability

The system allows voters and authorized entities to verify that all valid votes have been correctly recorded and tallied without compromising voter privacy. This feature discourages manipulation and enhances public confidence in the electoral process.

In addition to these core requirements, the system is designed to be efficient, flexible, and accessible via mobile platforms to improve availability and reliability. The system requirements are summarized in Figure 6.2

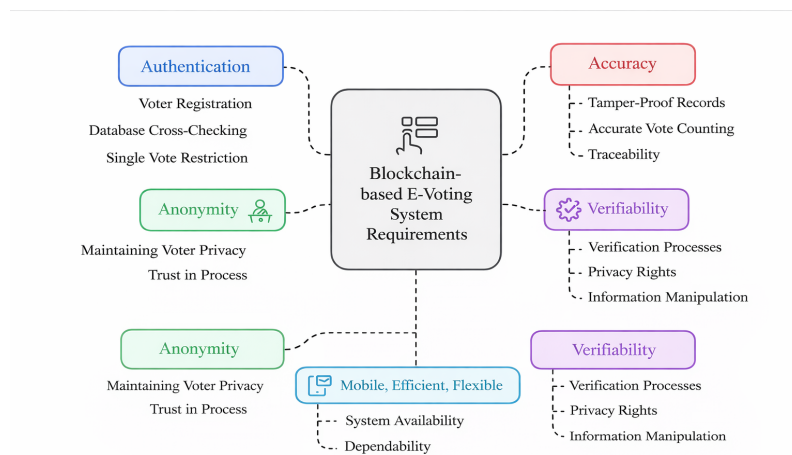


Figure 6.2: Requirements for a Blockchain-Based E-Voting System

6.2 Blockchain Implementation

All voting transactions are recorded on a blockchain, which forms the core of the proposed system.

6.2.1 Blockchain Structure

Each candidate is associated with a unique transaction identifier within the blockchain. The initial registration of a candidate establishes their public key. Subsequent votes are recorded as separate transactions linked to the respective candidate, creating a transparent and immutable vote ledger.

6.2.2 Voting Process

Voters interact with the system through a simple user interface to cast their votes. Each vote is recorded as a blockchain transaction, and the ledger is continuously updated as new votes are submitted.

6.2.3 Protest Vote

The system supports protest voting, allowing voters to submit a blank or neutral ballot to express rejection of all candidates or the political system. Vote chaining for multiple candidates is illustrated in Figure 6.3.

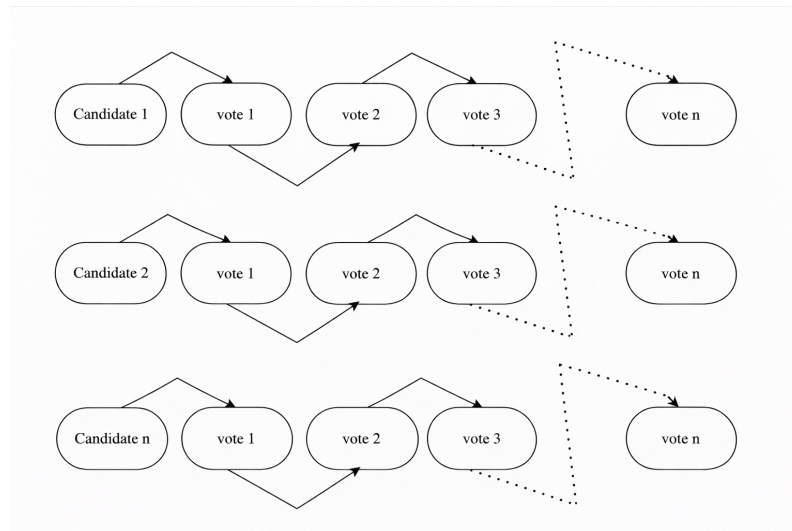


Figure 6.3: Vote Chaining for Multiple Candidates in a Blockchain System

6.2.4 Decentralization

Unlike centralized voting systems, blockchain decentralization ensures that no single authority controls the voting process. Each block is cryptographically linked to the previous block, making unauthorized data modification easily detectable.

6.3 Voting Process Steps

6.3.1 Requesting to Vote

Process: Voters initiate the voting process by submitting identifying information such as a jurisdiction-issued voter number, address, and a unique vote confirmation code.

Security: Submitted credentials are validated against a verified voter database. Invalid credentials are rejected, preventing multiple voting attempts and Sybil attacks.

6.3.2 Casting a Vote

Process: Voters select a preferred candidate or choose the protest vote option through a user-friendly interface. The vote casting workflow is illustrated in Figure 6.4.

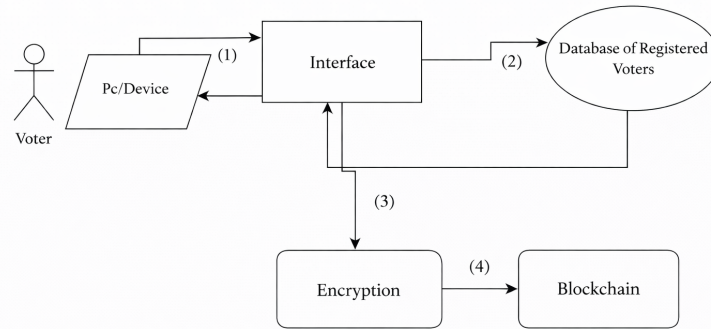


Figure 6.4: Blockchain-Based E-Voting Workflow: Voter to Blockchain Integration

6.3.3 Vote Encryption

Each vote is anonymized using the SHA-256 hashing algorithm. The hash is generated from a combination of the voter ID, selected candidate, and the hash of the previous vote. This ensures vote uniqueness, irreversibility, and voter privacy.

6.3.4 Including the Vote in the Blockchain

Process: The encrypted vote is added to the blockchain as a new transaction linked to the previous block.

Security: SHA-256 hashing guarantees data integrity and protects against voter identification or vote manipulation.

6.4 Conflict Resolution with Blockchain

The distributed nature of blockchain may lead to the creation of multiple competing blocks. The system resolves such conflicts using the *Longest Chain Rule*, a consensus mechanism also employed in Bitcoin.

6.4.1 Sybil Attacks and Blockchain Mitigation

Sybil attacks remain a challenge in distributed systems. As discussed by Douceur (2002), blockchain mitigates such threats through cryptographic validation and consensus mechanisms that limit the influence of malicious nodes.

6.4.2 Longest Chain Principle

When multiple blocks are generated concurrently (e.g., Blocks 1001-A, 1001-B, and 1001-C), the system temporarily selects one chain. The chain that continues to grow and accumulates the greatest computational effort becomes the primary chain. Competing blocks that are not extended are classified as orphan blocks and discarded. This process is illustrated in Figures 6.5 and 6.6.

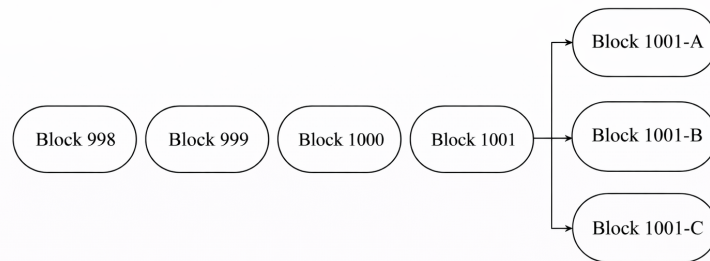


Figure 6.5: Forked Blockchain Representation: Main Chain and Diverging Blocks

6.5 Information Security and Cryptography

Reid and Harrigan (2013) demonstrated that blockchain transactions are pseudonymous rather than fully anonymous, and transaction graph analysis may reveal user identities. This study acknowledges these limitations and emphasizes the need for complementary anonymization techniques such as mix networks or zero-knowledge proofs.

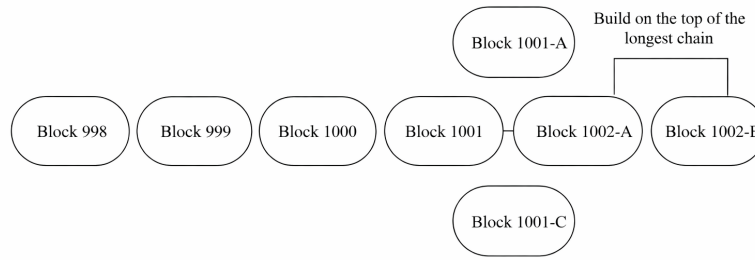


Figure 6.6: Conflict Resolution in Blockchain: Longest Chain Rule and Orphan Blocks

In the proposed system, each vote is encrypted using SHA-256, ensuring that voter data remains concealed within irreversible hash values. This approach preserves both voter anonymity and data integrity.

6.6 Experimental Design and Validation

To evaluate system feasibility, pilot experiments and controlled tests will be conducted.

6.6.1 Experimental Components

- **Sample Size:** A selected group of eligible voters
- **Blockchain Platform:** Ethereum, due to its smart contract support and Proof-of-Stake consensus
- **Evaluation Metrics:** Security, voter anonymity, transparency, auditability, and user satisfaction

6.6.2 Quantum-Resistant Security

To future-proof the system, quantum-resistant cryptographic techniques such as lattice-based encryption and hash-based signatures will be integrated to mitigate potential quantum computing threats.

6.7 Algorithmic Workflow and Flowcharts

The voting workflow follows these algorithmic steps:

1. Authentication Check

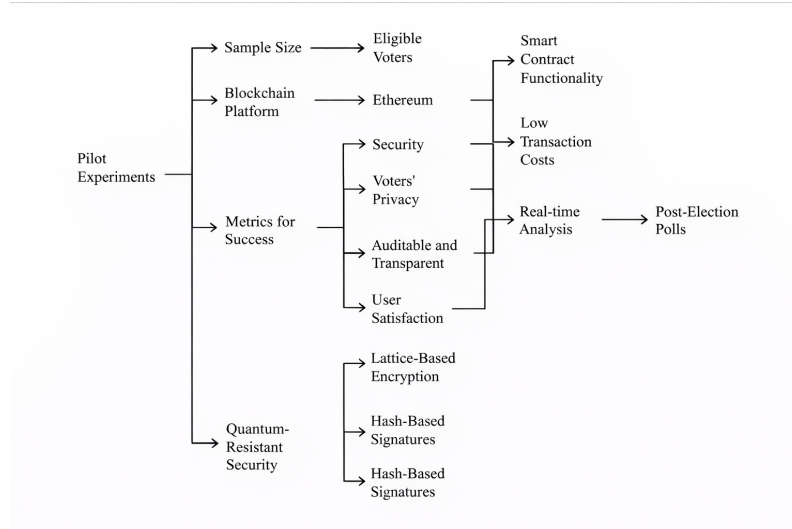


Figure 6.7: Pilot Design for Blockchain Voting Systems

2. Vote Casting
3. Vote Encryption using SHA-256
4. Blockchain Transaction Addition
5. Conflict Resolution using Longest Chain Rule
6. Vote Verification

6.7.1 Pseudo Code

BEGIN

FUNCTION authenticateVoter(voterID):

IF voterID EXISTS in VerifiedVoterList THEN

RETURN TRUE

ELSE

RETURN FALSE

END IF

FUNCTION castVote(voterID, candidateID):

IF authenticateVoter(voterID) THEN

RETURN candidateID

ELSE

RETURN "Authentication Failed"

END IF

FUNCTION encryptVote(vote, voterID, prevHash):

voteData ← CONCAT(vote, voterID, prevHash)

```
    encryptedVote ← SHA256(voteData)
    RETURN encryptedVote

FUNCTION createBlock(encryptedVote):
    newBlock ← {
        voteHash: encryptedVote,
        previousHash: GET_PREVIOUS_HASH(),
        timestamp: GET_CURRENT_TIME()
    }
    RETURN newBlock

FUNCTION addToBlockchain(block):
    blockchain.APPEND(block)

FUNCTION resolveConflicts():
    blockchain ← FIND_LONGEST_CHAIN(blockchain)

FUNCTION verifyVote(voterID):
    FOR block IN blockchain:
        IF block.contains(voterID) THEN
            RETURN block.voteHash
        END IF
    END FOR
    RETURN "Vote Not Found"
END
```

6.8 Summary

This methodology demonstrates a systematic approach to implementing a secure, transparent, and verifiable blockchain-based e-voting system. By combining decentralized control, cryptographic protection, and robust conflict resolution mechanisms, the proposed system addresses key weaknesses of traditional electronic voting systems and presents a scalable solution suitable for future democratic processes.

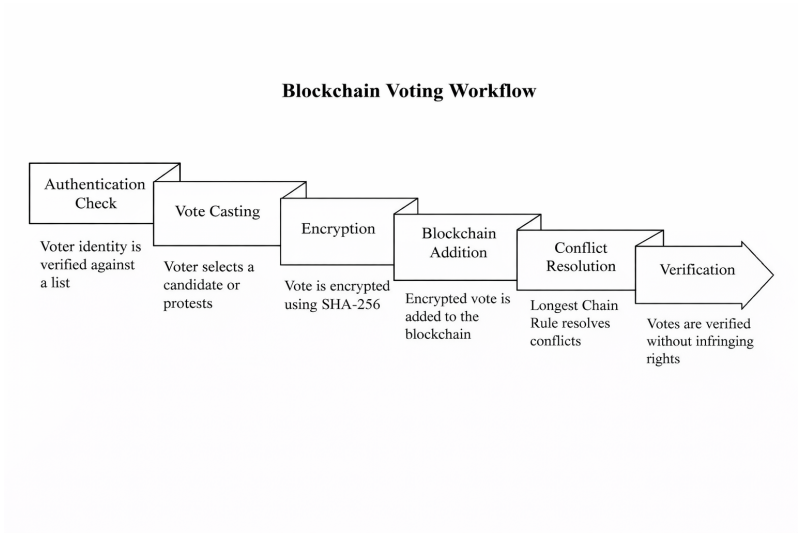


Figure 6.8: Blockchain Voting Workflow

Chapter 7

Prototype Testing

Analyzing the e-voting system prototype, one can note that it adapts blockchain technology to ensure the security and transparency of votes. The way the prototype works is divided into sub screenshots presented below. The major functions are the following four:

(Voter Audit Demonstration Auditability of decentralized voting implies the production of these permanently secure and tamper-resistant records which can be reviewed by anybody. In a blockchain-based system your vote is registered as a cryptic transaction. Such a transaction will still be reflected in the public ledger, but it will be able to conceal your personal information by keeping the true identities of voters and candidates encrypted. The new hash of the previous hash and voter and candidate ID is put into every record in order to demonstrate that one was not tampered with. The integrity of the blockchain is absolutely clear since the new hash points to the older one.)

1. **Vote selection:** The screenshot indicates an initial stage when voters select the party on the list and enter their voter ID. This interface is easy to use since you can choose a party using a drop-down and input your voter ID, such as VOID001, which is an item selected among a list of sample IDs. This action makes the voting secure.

[evoting system using Blockchain](#)

Select Political party to vote		select
Enter Voter ID (enter from sample Voter ID)		VOID001
		Vote

Request to mine | Resync | View Chain

Sample Voter ID
VOID001
VOID002
VOID003
VOID004
VOID005

Result Detail		
Voter ID	Political Party Name	Voted Time

Result Summary	
Political Party Name	Total vote gain
Party: A	0
Party: B	0
Party: C	0
Party: D	0

Figure 7.1: Vote Selection

2. **Blockchain mining:** The voting data is added to a block in the blockchain as seen displayed on the second screenshot. This step provides transparency since each

block contains a timestamp and a value that cannot be changed called a hash value allowing the voters to verify the authenticity of the results.



Figure 7.2: Blockchain Mined

3. **Tracking results:** In the third screenshot, the user clearly sees in real-time how many votes are included in the vote. In this case, it is observed that the Democratic Party has 5 votes as compared to the Republican Party with 2 and Socialist Party with 0 votes.

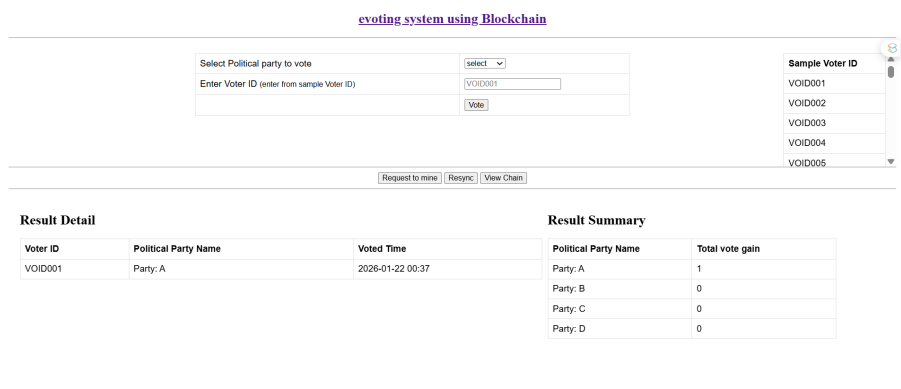


Figure 7.3: Tracking Results

4. **Results publishing:** The fourth screenshot is a zoom of the blockchain chain observation, which shows every transaction in the trail. We will be able to notice voter ID, political party, and time-stamp of each vote. Such a blockchain arrangement will ensure transparency and accountability, and everyone can check that the election is fair and unaltered. With the help of this technology, the authenticity of the results can be proven by anyone.
5. **Results Summary:** As you scroll down to the last screenshot, you can peep at an illumination on the final figure. It is continuously changing and therefore displays the accurate amount of votes each party has filled in as the voting doors shut. The Democratic party secured 5, the Republican 2 votes and the Socialist Party ended

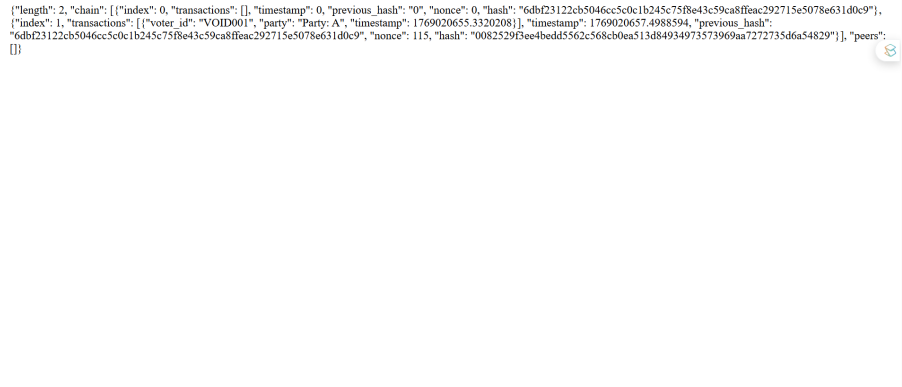


Figure 7.4: Longest Chain with Hash and data

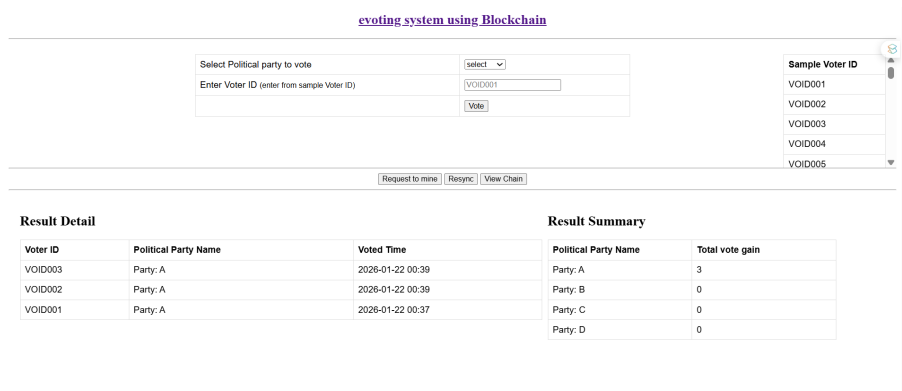


Figure 7.5: Results Summary

up with 0. Having this real time tally on the front page, a viewer can track the outcomes as they come in -no more waiting until the late night news to see who is leading.

Within this prototype, blockchain technology as applied to an e-voting system seeks to enhance some important features:

1. Usability Improvements

Improves the user experience by increasing the intuitive and accessible nature of the voting applications.

2. SHA-256 Encryption

Ensures that the integrity and security of a vote cast is guaranteed and cannot be tampered with.

3. Transaction History

Offers transparency as well as auditability and does not sacrifice voter privacy.

4. PoS Ethereum Consensus

The system-Scales it to process a large volume of transactions relating to voting.

5. Longest Chain Rule

Deterrence against vote fraud by making sure that the chain with the most points wins, meaning chain forks will not have conflicts.

6. Zero-Knowledge Proofs

Guards the privacy and anonymity of a voter, so his/her data will be confidential, but not the system.

7. Predefined User Scalability

The system can accommodate more users and the more users you add to it the more you add predefined users in the code making the expansion of the system seamless and still perform effectively.

Chapter 8

Limitation & Challenges

8.0.1 Limitations

Modern e-voting in Bangladesh faces major obstacles that Blockchain technology introduces as barriers to adoption.

1. Insufficient internet connectivity in Bangladesh's rural poverty regions creates an adoption barrier that hinders system adoption throughout the nation. A lack of experts with blockchain technology experience stands as a primary obstacle to both creating and supporting the system.
2. Holding insufficient digital literacy by voters leads to pessimism about electoral tech creating social obstacles in the voting process. The risk of election unfairness arises from political maneuvers while voters try to protect their electoral secrecy.
3. An open legal structure regarding blockchain-based voting must exist in Bangladesh to provide standard guidelines which ensure election process transparency. The implementation of blockchain encounters two essential problems: an absence of thorough cybersecurity legislation and a lack of capability to merge electoral systems with current infrastructure.

Bangladesh needs to tackle its technical and legal problems NOW to make blockchain-based e-voting successful.

8.0.2 Challenges

1. constraints in the availability of Internet facilities

Challenge: Currently, more internet users are reported to be living in urban areas compared to people in rural and semi-urban areas. Approximately, about 43% of the population of Bangladesh has proper internet connectivity as surveyed by Bangladesh Telecommunication Regulatory Commission in 2023.

Impact on E-Voting: Again, blockchain-based voting is carried out through the

completion of transactions on the internet without physical interaction. Lack of infrastructure might leave a significant share of the population displaced which in turn causes variation in the voting process.

Proposed Solution: Design a mobile voting application that is low bandwidth and integrates blockchain. Telecom partners could help in increasing 4G/5G networks in rural areas during the election periods.

2. Lack of skilled human resource in the blockchain industry

Challenge: Blockchain is a young technology in Bangladesh, and there is little to no local talent for its implementation in this country. The problem of dearth of skilled blockchain professionals was also underscored in a 2024 report by the BASIS (Bangladesh Association of software and information services).

Impact on E-Voting: Lack of expertise is an unambiguous way of exposing certain systems due to an improper implementation of the system.

Proposed Solution: Seek partnership with foreign based blockchain organizations that will erect local professionals. They should also bring courses that are aligned with blockchain to ensure an academic institution churns out a skilled workforce in the future.

3. Further, general lack of legal and regulatory framework.

Challenge: There is no regulatory legislation on blockchain solutions, including voting systems in Bangladesh. The current laws governing the elections together with the IT laws have shortcomings to a certain extent regarding legal tenders, juridical signatures within the election processes.

Impact on E-Voting: Outright lack of regulations slow down the process of implementation of blockchain voting system and leave room for legal battles over who won the election.

Proposed Solution: The special guidelines and regulations of blockchain voting should be prepared with the help of the Ministry of ICT, and the Election Commission of Bangladesh (ECB) should work with the Ministry on this issue. Such may involve standards that regard the process of vote encryption, voter registration procedures, and ways in which such conflicts would be solved.

4. Resistance from Stakeholders

Challenge: Decision makers and elections officers who have dealt with established methods in prior years will not be inclined towards using blockchain because of increased complexities and openness. Political parties may also mistrust new technology because of fear that their messages will be breached or altered.

Impact on E-Voting: They feared that resistance might hinder the implementation processes and ultimately the public might lose confidence in the system.

Proposed Solution: Fix awareness campaigns and do pilot tests to evidence the safety and effectiveness of using blockchain for voting. Some transparency activ-

ities for instance, the past, present or future audit outcomes increase stakeholder confidence.

5. High Initial Costs

Challenge: Blockchain implementation assumes the costs relating to the acquisition of the necessary hardware and creation of the software and training of personnel. The Bangladesh government gives a relatively meagre amount towards electoral reforms as revealed by the 2023 Policy Research Institute of Bangladesh.

Impact on E-Voting: The problem is that policymakers may be discouraged by the high initial costs of such systems, despite that blockchain systems, in the long run, help to decrease election fraud and the usage of paper.

Proposed Solution: Preliminary financing needs to be sought in a similar way from international organizations such as World Bank or UNDP. The Other Way through which the government could ease the burden is by Facilitate Public-Private Partnerships.

6. Security and Privacy Concerns

Challenge: Despite the untouchable security which blockchain provides, it is vulnerable to more advanced cyber threats such as quantum computing and Sybil. As per the Global Cybersecurity Index index 2022 Bangladesh's cybersecurity facility is weak.

Impact on E-Voting: Weak implementation of security measures may lead to a breach of such a system and consequent loss of confidence from the public.

Proposed Solution: Buy out quantum-vulnerable cryptography and follow secure protocols for information technology. Evaluation involving the best cybersecurity firms from across the world could improve the firm's system.

Chapter 9

Conclusion

Therefore, the above proposed blockchain implemented e-voting system consists of favourable traits to overcome some of the prevailing flaws that are particularly associated with the conventional e-voting system. While pilot testing reveals the improved system capability, availability of Cryptography, and ease of use and attractiveness of interface, challenges include limited infrastructural support, high costs and the need for set up regulatory rules. The future research should focus on eradicating such factors – enhance the efficiency of blockchain, make it available for the underdeveloped nations, and establish the right legal environment. More work is also needed to address newcomers such as a quantum computing attack, and to expand the research on the model that demonstrates the effectiveness of combining the public and private blockchains for the greatest security and performance. Such measures will be helpful as doublings to achieve the aim of cryptography in giving secure and effective electoral framework internationally.

References

- [1] Madise and T. Martens, “E-voting in estonia 2005: The first practice of country-wide binding internet voting in the world,” in *Electronic Voting, 2nd International Workshop*, Bregenz, Austria, Aug. 2006.
- [2] V. Yedhukrishnan, V. S. Nanditha, N. K. Biju, and F. Sali, “A survey on e-voting systems using blockchain,” 2024. [Online]. Available: <https://ijera.in/archive/volume%204%20issue%201/NACORE%20P129.pdf>
- [3] S. S. Kolte, A. Sudarshan, and C. Shree, “Decentralized and secure voting system using blockchain technology,” 2023. [Online]. Available: <https://www.researchgate.net/publication/382180564>
- [4] T. Chafiq, R. Azmi, and O. Mohammed, “Blockchain-based electronic voting systems: A case study in morocco,” *International Journal of Intelligent Networks*, vol. 5, 2024.
- [5] A. Johari, K. Dhall, and A. Vasudeva, “E-voting system based on blockchain technology,” 2024. [Online]. Available: <http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/11430/1/E-Voting%20System%20based%20on%20Blockchain%20Technology.pdf>
- [6] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [7] S. Raval, *Decentralized Applications: Harnessing Bitcoin’s Blockchain Technology*. Sebastopol, CA: O’Reilly Media, 2016.
- [8] National Institute of Standards and Technology, “Federal information processing standards publication,” 2012.
- [9] I. S. G. Stenerud and C. Bull, “When reality comes knocking: Norwegian experiences with verifiable electronic voting,” in *Electronic Voting*, vol. 205, 2012, pp. 21–33.
- [10] “New south wales ivote system,” *International Journal of Network Security & Its Applications*, vol. 9, no. 3, 2017.
- [11] “D.c digital vote-by-mail service,” *International Journal of Network Security & Its Applications*, vol. 9, no. 3, 2017.

-
- [12] D. Chaum, “Blind signatures for untraceable payments,” in *Advances in Cryptology*, 1983.
- [13] L. Gupta, P. Srivastava, and P. K. Gupta, “Secure e-voting system using blockchain,” 2024. [Online]. Available: <http://www.ir.juit.ac.in:8080/jspui/bitstream/123456789/11418/1/Secure%20E-Voting%20System%20using%20Blockchain.pdf>
- [14] S. Laia and A. M. Barmawi, “Strengthening the authentication mechanism of blockchain-based e-voting system using post-quantum cryptography,” *Journal of Informatics*, 2024. [Online]. Available: <https://join.if.uinsgd.ac.id/index.php/join/article/view/1305>
- [15] “Vote casting process in the estonian i-voting system,” *International Journal of Network Security & Its Applications*, vol. 9, no. 3, 2017.
- [16] Luxoft, “Report on switzerland’s first blockchain-based vote reveals citizens want more e-voting,” 2024, accessed: 24-Jan-2026. [Online]. Available: <https://www.luxoft.com/pr/report-on-switzerlands-first-blockchainbased-vote-reveals-citizens-want-more-evoting>
- [17] J. Gerlach and U. Grasser, “Three case studies from switzerland: E-voting,” Berkman Center for Internet & Society, Tech. Rep., 2009.
- [18] C. Meter, A. Schneider, and M. Mauve, “Tor is not enough: Coercion in remote electronic voting systems,” 2017, arXiv preprint.
- [19] KMD, “Internet voting pilot to be discontinued,” 2014, accessed: Feb. 25, 2025. [Online]. Available: <https://www.regjeringen.no/en/historical-archive/solbergs-government/Ministries/kmd/press-releases/2014/Internet-voting-pilot-to-be-discontinued/id764300/>
- [20] J. A. Halderman and V. Teague, “The new south wales ivote system: Security failures and verification flaws in a live online election,” in *International Conference on E-Voting and Identity*, 2015, pp. 35–53.
- [21] S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, “Attacking the washington, dc internet voting system,” in *International Conference on Financial Cryptography and Data Security*, 2012, pp. 114–128.
- [22] F. Reid and M. Harrigan, “An analysis of anonymity in the bitcoin system,” in *Security and Privacy in Social Networks*, 2013, pp. 1–27.
- [23] J. R. Douceur, “The sybil attack,” in *International Workshop on Peer-to-Peer Systems*, 2002, pp. 251–260.
- [24] Bangladesh Telecommunication Regulatory Commission, “Internet user statistics 2023,” 2023, accessed: Jan. 23, 2026. [Online]. Available: <https://www.btrc.gov.bd>

- [25] Bangladesh Association of Software and Information Services, “Annual industry report 2024,” 2024, accessed: Jan. 23, 2026. [Online]. Available: <https://basis.org.bd>
- [26] International Telecommunication Union, “Global cybersecurity index 2022,” 2022, accessed: Jan. 23, 2026. [Online]. Available: <https://www.itu.int>
- [27] National Institute of Standards and Technology, “Advances in post-quantum cryptography,” 2023, accessed: Jan. 23, 2026. [Online]. Available: <https://www.nist.gov>
- [28] S. Muruges and A. Jeyasekar, “A blockchain-based liquid democracy voting system using ethereum,” *Journal of Distributed Ledger Technology*, 2024.