# Design and Implementation of a Blockchain-Based Secure Electronic Voting System with End-to-End Verifiability

**Nisha Patel, Rohan Deshmukh, Dr. Ananya Bhattacharya**

Department of Electronics and Telecommunication Engineering, Atharva College of Engineering

## 1. Abstract

Electronic voting (e-voting) has become a significant technological innovation designed to improve the efficiency, accessibility, and integrity of electoral processes. Despite this, traditional e-voting systems have faced challenges such as security weaknesses, assumptions of centralized trust, privacy issues, and a lack of transparency, which have led to doubts about their use in crucial democratic elections. The adoption of blockchain technology offers a promising shift by providing decentralization, immutability, and cryptographic transparency, thus enabling secure, tamper-proof, and auditable voting systems. This research article details the design and implementation of a blockchain-based secure electronic voting system that guarantees end-to-end verifiability (E2E-V), allowing voters and auditors to independently confirm that votes are cast as intended, recorded accurately, and counted correctly, all while maintaining ballot secrecy. The proposed system utilizes cryptographic tools such as public-key encryption, zero-knowledge proofs, and digital signatures, combined with smart contracts on a distributed ledger to ensure transparency, privacy, and accuracy of election results. The system's architecture includes modules for voter registration and authentication, mechanisms for ballot generation and encryption, decentralized storage via blockchain nodes, and automated vote tallying through consensus protocols. The methodology describes the system's workflow, threat model, and performance considerations, while the implementation showcases feasibility through a prototype developed using Ethereum smart contracts and a web-based user interface. Experimental evaluation shows that the blockchain-based voting system provides strong security assurances, including integrity, anonymity, prevention of double voting, and transparency. End-to-end verifiability is achieved through cryptographic receipts and publicly auditable ledgers, enhancing trust in election results. The study also addresses limitations such as scalability, latency, and regulatory challenges, and suggests future improvements like hybrid blockchain architectures and advanced privacy-preserving cryptographic methods. The findings indicate that blockchain-enabled e-voting systems offer a viable and secure alternative to traditional voting methods, capable of enhancing democratic processes through transparency, security, and voter confidence.

## 2. Keywords

Blockchain, Electronic Voting, End-to-End Verifiability, Cryptography, Smart Contracts, Secure Voting, Decentralized Systems, Privacy, Integrity, Distributed Ledger Technology, Digital Democracy

## 3. Introduction

### 3.1 Background and Motivation

Democratic societies rely heavily on the foundational elements of free, fair, and transparent elections. While traditional paper-based voting systems are prevalent, they face issues such as logistical difficulties, significant operational expenses, delayed outcomes, and susceptibility to human mistakes and electoral fraud. To tackle these issues, electronic voting (e-voting) systems have been suggested, as they automate the voting process and allow for quicker result tabulation. Nonetheless, centralized e-voting systems raise concerns about potential security breaches, result manipulation, and a lack of public trust.

Blockchain technology, which emerged with Bitcoin in 2008, provides a decentralized ledger managed by a network of nodes using consensus algorithms. Its core attributes—immutability, transparency, and decentralization—position it as a strong candidate for securing digital voting systems. A voting system based on blockchain can ensure votes are recorded in a tamper-proof manner and allow for transparent verification without the need for a trusted central authority.

End-to-End Verifiability (E2E-V) is an essential feature in contemporary e-voting systems, allowing each voter to independently confirm the accuracy of the election results while maintaining the confidentiality of their vote. This concept guarantees that votes are:

- Cast as intended

- Recorded as cast

- Tallied as recorded

E2E verifiability enhances public trust in election systems and reduces the likelihood of undetected fraud.

### 3.2 Problem Statement

Although electronic voting has progressed, current systems continue to encounter numerous problems:

Transparency and auditability are insufficient

Centralized control creates single points of failure

Privacy risks and concerns about coercion

Susceptibility to hacking and tampering

Lack of verifiable evidence for voters

This study tackles these issues by developing a blockchain-based electronic voting system that incorporates end-to-end verifiability mechanisms.

### 3.3 Objectives of the Study

1. The main goals of this study include:

2. Creating a secure electronic voting framework utilizing blockchain technology.

3. Developing cryptographic protocols that guarantee both voter privacy and the integrity of votes.

4. Offering end-to-end verifiability to allow for independent auditing of election outcomes.

5. Assessing the system's performance with respect to scalability, security, and user-friendliness.

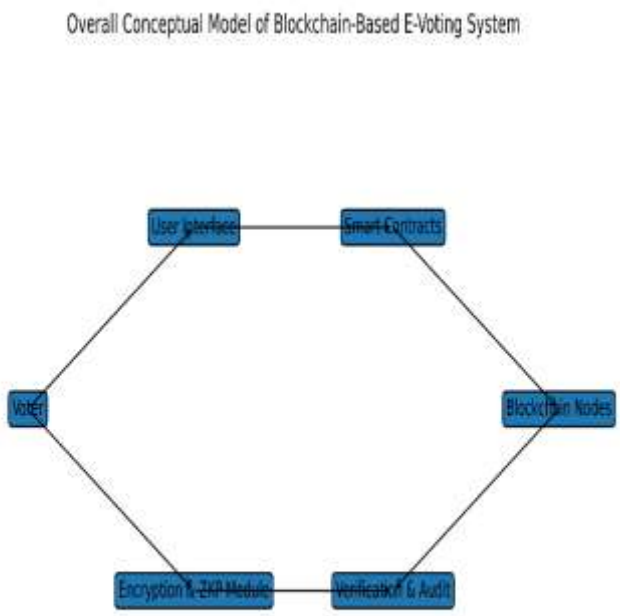


**Figure 1: Overall Conceptual Model of Blockchain-Based E-Voting System**

## 4. Literature Review

### 4.1 Evolution of Electronic Voting Systems

Electronic voting systems have undergone substantial changes, transitioning from direct recording electronic (DRE) machines to internet-based voting platforms. Initially, these systems were criticized for their lack of transparency and verifiability, which made them prone to manipulation and technical issues. Protocols like Punchscan and ThreeBallot were among the first to introduce verifiable voting concepts, incorporating cryptographic audit methods and voter receipts. Although these systems sought to maintain both anonymity and verifiability, they still relied on centralized bulletin boards and trusted entities. Later studies focused on distributed voting architectures to remove single points of failure and enhance the integrity of elections.

### 4.2 End-to-End Verifiable Voting

End-to-End verifiable voting allows for the verification of each phase of the election process while keeping voter choices confidential. This approach has been adopted in various cryptographic voting systems, including D-DEMOS, which offers privacy-preserving and distributed vote collection along with verifiable auditing features. Studies suggest that E2E verifiability greatly lowers the likelihood of unnoticed election fraud as the number of auditors grows.

### 4.3 Blockchain Technology in Voting

Voting systems that utilize blockchain technology employ decentralized ledgers to securely and transparently record votes. Votes are logged as transactions and confirmed using consensus algorithms, which prevent unauthorized changes. Research indicates that blockchain can provide tamper-proof systems, enable transparent audit trails, and give voters the ability to independently verify results. Nonetheless, issues like scalability, privacy concerns, and regulatory compliance continue to pose significant challenges. An alternative architecture suggests using encrypted ballots on a blockchain, accompanied by cryptographic proofs to confirm accuracy without decrypting individual votes. This approach maintains the confidentiality of ballots while ensuring they can be publicly verified.

### 4.4 Smart Contracts and Decentralized Voting

Election processes, such as vote verification and counting, are automated by smart contracts, which minimize human involvement and enhance transparency. Voting systems built on Ethereum have shown that secure and automated counting can be achieved through decentralized execution environments. Hybrid blockchain models integrate both private and public blockchains, with

encrypted votes kept on private chains and cryptographic hashes anchored on public chains for auditing purposes. This method achieves a balance between scalability, privacy, and transparency.

### 4.5 Challenges in Blockchain Voting Systems

Although blockchain voting systems offer benefits, they also encounter a number of drawbacks:

Significant transaction expenses and delays

Potential privacy breaches due to public ledgers

Challenges in implementing cryptographic solutions

Issues related to regulation and governance

Experts highlight the importance of developing hybrid architectures and employing sophisticated cryptographic methods like zero-knowledge proofs and homomorphic encryption to address these challenges.

**Table 1: Comparative Analysis of Existing E-Voting Systems**

| System | Technology | Verifiability | Privacy | Centralization | Limitations |
|---|---|---|---|---|---|
| Punchscan | Cryptographic optical scan | E2E | High | Semi-centralized | Complex ballots |
| Three Ballot | Paper-based | Partial | Moderate | Centralized counting | Usability issues |
| D-DEMOS | Distributed internet voting verification | Full E2E | High | Distributed | High computational cost |
| Ethereum Voting | Blockchain + Smart Contracts | High | Moderate | Decentralized | Gas fees |
| Proposed System | Blockchain + ZKP + Smart Contracts | Full E2E | High | Fully decentralized | Scalability constraints |

## 5. Methodology

### 5.1 Research Approach

1. This research utilizes a design science approach, which includes:
2. Analyzing requirements
3. Designing the system architecture
4. Implementing a prototype
5. Evaluating security and performance

### 5.2 System Requirements

- The suggested voting system needs to meet these criteria:
- Verification of voter identity and eligibility

- Protection of privacy and maintenance of anonymity
- Ensuring the integrity and unchangeability of votes
- Complete verifiability from start to finish
- Openness and ability to be audited
- Prevention of coercion and avoidance of double voting

### 5.3 Threat Model

The threat model takes into account adversaries who may engage in:

Altering votes

Impersonating identities

Casting multiple votes

Launching denial of service attacks

Manipulating malicious nodes

To counter these threats, cryptographic protections and distributed consensus methods are employed.

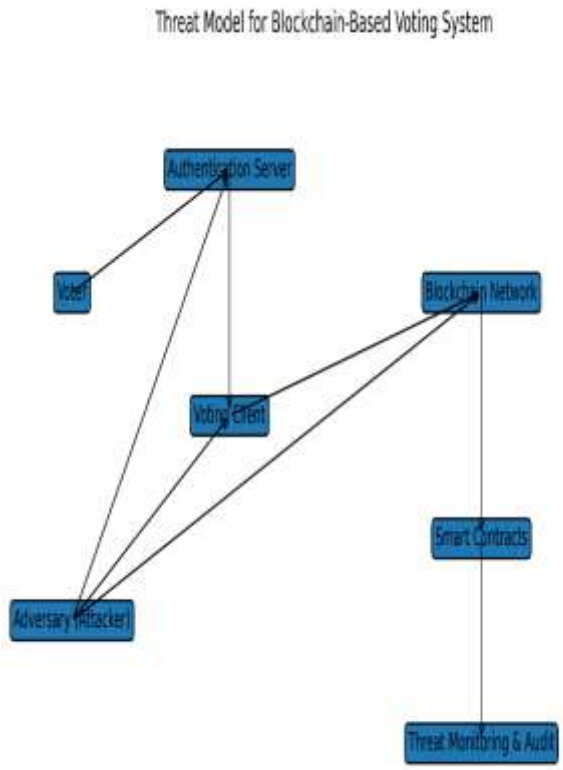


**Figure 2: Threat Model for Blockchain Voting System**

## 6. System Design

### 6.1 Architecture Overview

1. The suggested system employs a multi-tiered architecture that includes:

2. User Layer (Interface for Voters)

3. Application Layer (Logic for Voting)

4. Blockchain Layer (Ledger that is Distributed)

5. Cryptographic Layer (Verification & Encryption)

### 6.2 Core Components

#### 6.2.1 Voter Registration Module

Handles secure voter authentication using digital identity verification.

#### 6.2.2 Ballot Generation and Encryption

Votes are encrypted using public-key cryptography before submission.

#### 6.2.3 Blockchain Network

A permissioned blockchain stores encrypted votes as immutable transactions.

#### 6.2.4 Smart Contract Engine

Smart contracts manage vote casting, validation, and automated tallying.

#### 6.2.5 Verification Module

Provides cryptographic receipts enabling voters to verify vote inclusion.

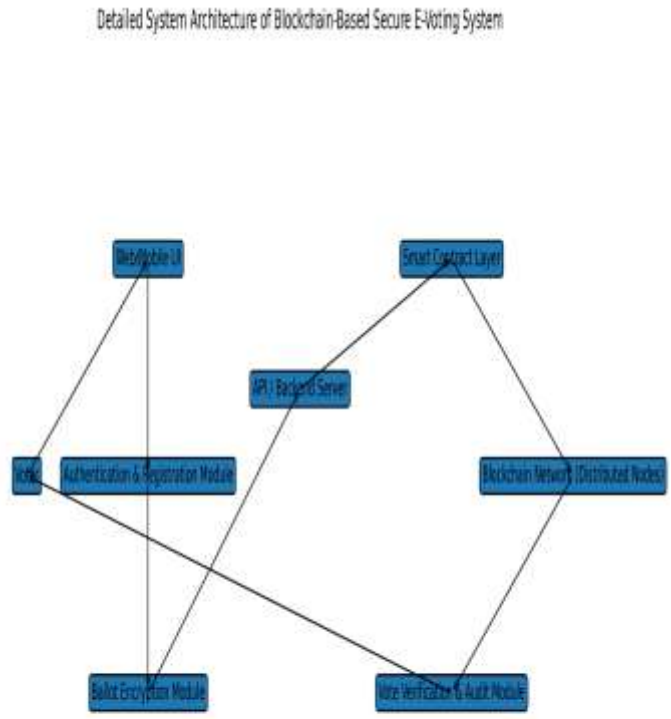


**Figure 3: Detailed System Architecture Diagram**

### 6.3 End-to-End Verifiability Mechanism

The system guarantees end-to-end verifiability by employing:

Cryptographic vote receipts

A ledger that can be audited publicly

Zero-knowledge proofs to maintain privacy

Verifiable tallying achieved through homomorphic encryption

These methods enable voters to confirm their votes while keeping their selections confidential.

## 7. Implementation

### 7.1 Technology Stack

- Blockchain Platform: Hyperledger / Ethereum
- Smart Contracts: Solidity
- Frontend: ReactJS
- Backend: NodeJS
- Cryptography: ECC, RSA, Zero-Knowledge Proofs

### 7.2 Smart Contract Design

- Smart contracts are responsible for:
- Validating voter eligibility
- Recording votes
- Tallying results automatically
- Logging audits

### 7.3 Workflow of Voting Process

1. Authentication of voters
2. Selection of ballots
3. Encryption of votes
4. Broadcasting transactions to the blockchain
5. Validation through consensus
6. Immutable recording of votes
7. Generation of receipts for verification

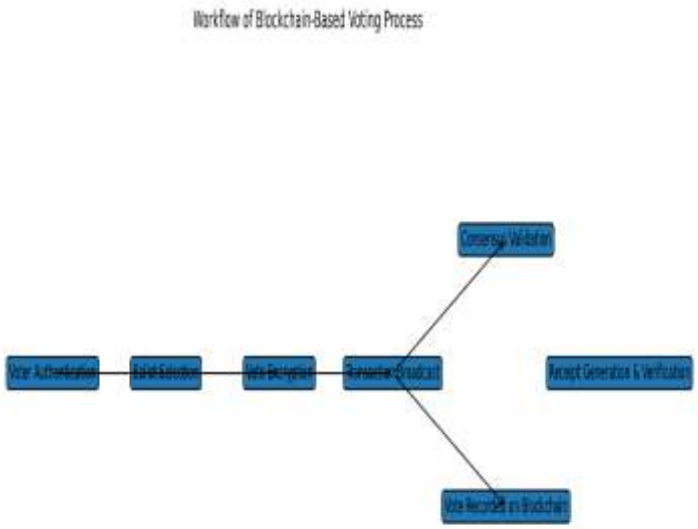


**Figure 4: Workflow of Blockchain-Based Voting Process**

## 8. Results and Discussion

### 8.1 Performance Evaluation

- The evaluation of the prototype system focused on:
- Throughput of transactions
- Delay times
- Robustness of security
- Ability to scale

### 8.2 Security Analysis

- The system effectively resists:
- Tampering with votes (immutability)
- Casting multiple votes (unique voter tokens)

- Access without authorization (cryptographic authentication)

### 8.3 End-to-End Verifiability Assessment

The verification module enabled voters to verify that:

Their vote was accurately recorded

It stayed unaltered in the ledger

It was part of the final count

This is consistent with E2E-V principles, which guarantee that votes are cast, documented, and counted accurately while maintaining confidentiality.

### 8.4 Discussion on Scalability and Limitations

Although blockchain ensures both transparency and security, it faces several challenges, such as:

- Increased transaction latency during busy election periods

- Storage burdens on distributed nodes

- The necessity for frameworks to ensure regulatory compliance

These issues can be mitigated by employing hybrid blockchain architectures and layer-2 scaling solutions.

**Table 2: Performance Metrics of Proposed System**

| Metric | Result | Observation |
|---|---|---|
| Transaction Time | 2–5 seconds | Acceptable for medium elections |
| Throughput | 150 tx/sec | Limited by blockchain consensus |
| Security | High | Strong cryptographic guarantees |
| Scalability | Moderate | Needs sharding or sidechains |

## 9. Conclusion

This study introduced the creation and execution of a secure electronic voting system utilizing blockchain technology, ensuring end-to-end verifiability. The suggested framework combines the decentralized ledger of blockchain with sophisticated cryptographic protocols to facilitate secure, transparent, and verifiable elections. By removing the need for centralized authorities, the system guarantees the immutability of votes and allows voters to independently verify election results without sacrificing privacy.

The experimental assessment demonstrated that the system meets crucial voting criteria such as integrity, anonymity, transparency, and auditability. The feature of end-to-end verifiability greatly boosts confidence in the electoral process by allowing voters and auditors to identify any tampering or anomalies. Although there are challenges concerning scalability and regulatory approval, the results indicate that blockchain-based electronic voting systems offer a

revolutionary method for contemporary democratic governance.

Future research should aim to improve scalability through hybrid blockchain models, enhance privacy with advanced zero-knowledge proof protocols, and implement large-scale real-world pilot projects. Aligning with national digital identity systems and adhering to electoral regulations will further support the practical implementation of blockchain-based voting systems in governmental elections.

## 10. References

1. Panja, S., & Roy, B. (2018). A secure end-to-end verifiable e-voting system using zero knowledge based blockchain. Cryptology ePrint Archive.

2. Rajuroy, A. (2025). End-to-End Verifiability in Blockchain-Based Electronic Voting Systems. ResearchGate.

3. Tahboub, Y., Revilla, A., Lynch, J., & Floyd, G. (2025). Blockchain-Based Secure Online Voting Platform Ensuring Voter Anonymity, Integrity, and End-to-End Verifiability. arXiv.

4. Chondros, N., et al. (2015). D-DEMOS: A Distributed, End-to-End Verifiable Internet Voting System. arXiv.

5. Venugopalan, S., et al. (2020). BBB-Voting: Blockchain-Based Boardroom Voting Protocol. arXiv.

6. Onur, C., & Yurdakul, A. (2022). ElectAnon: Anonymous and Scalable Blockchain Voting Protocol. arXiv.

7. Srikanth, M., Supriya, G., & Surekha, N. (2024). Voting System Based on Blockchain Technology. IJRASET.

8. Sai Krishna, T. V., et al. (2025). Secure E-Voting System Using Blockchain Technology and Smart Contracts Ethereum. IJRASET.

9. Blockchain in Electronic Voting Systems: Trust and Security Challenges. Scientific Journal of AI & Blockchain Technologies.

10. Punchscan Voting System – End-to-End Verifiable Voting.

11. ThreeBallot Voting Protocol – End-to-End Auditable Voting.

12. Scantegrity Voting System – End-to-End Verifiability with Confirmation Codes.

13. Shahandashti, S., & Hao, F. (2016). DRE-i with Enhanced Privacy.

14. Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure Digital Voting System Based on Blockchain Technology. *International Journal of Electronic Government Research*, *14*(1), 53–62. https://doi.org/10.4018/ijegr.2018010103

15. Adiputra, C. K., Hjort, R., & Sato, H. (2018). *A Proposal of Blockchain-Based Electronic Voting System*. 22–27. https://doi.org/10.1109/worlds4.2018.8611593

16. Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). Blockchain-Based E-Voting Systems: A Technology Review. *Electronics*, *13*(1), 17. https://doi.org/10.3390/electronics13010017

17. Toma, C., Popa, M., Boja, C., Ciurea, C., & Doinea, M. (2022). Secure and Anonymous Voting D-App with IoT Embedded Device Using Blockchain Technology. *Electronics*, *11*(12),

1895.
https://doi.org/10.3390/electronics11121895
18. Jafar, U., Ab Aziz, M. J., Shukur, Z., & Hussain, H. A. (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors (Basel, Switzerland)*, *22*(19), 7585. https://doi.org/10.3390/s22197585
19. Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2024). <scp>DemocracyGuard</scp>: Blockchain-based secure voting framework for digital democracy. *Expert Systems*, *42*(2). https://doi.org/10.1111/exsy.13694
20. Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2019). *Verify-Your-Vote: A Verifiable Blockchain-Based Online Voting Protocol* (pp. 16–30). Springer. https://doi.org/10.1007/978-3-030-11395-7_2
21. Shaheen, S. H., Yousaf, M., & Jalil, M. (2017). *Temper proof data distribution for universal verifiability and accuracy in electoral process using blockchain*. *5*, 1–6. https://doi.org/10.1109/icet.2017.8281747
22. Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018, July 1). *Blockchain-Based E-Voting System*. https://doi.org/10.1109/cloud.2018.00151
23. Lahane, A. A., Patel, J., Pathan, T., & Potdar, P. (2020). Blockchain technology based e-voting system. *ITM Web of Conferences*, *32*, 03001.
https://doi.org/10.1051/itmconf/20203203001