Gourav Singh, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Blockchain-Based Voting System Enhancing Electoral Security, Transparency, and Accessibility Through Decentralized Technology

Gourav Singh[1], Arjun Pataskar[2]
[1]B.Tech CSE, Parul Institute of Technology, Parul University, Vadodara, India
[2]B.Tech CSE, Parul Institute of Technology, Parul University, Vadodara, India

Abstract- The integrity of electoral systems is fundamental to democratic governance; however, traditional voting mechanisms suffer from security vulnerabilities, lack of transparency, and accessibility constraints. This paper proposes a blockchain-based voting system leveraging distributed ledger technology to ensure secure, transparent, and tamper-resistant elections. The system integrates cryptographic techniques such as Zero-Knowledge Proofs (ZKPs) and Elliptic Curve Cryptography (ECC) within a permissioned blockchain framework using Hyperledger Fabric and Practical Byzantine Fault Tolerance (PBFT) consensus. A three-tier architecture consisting of Application, Blockchain, and Data Storage layers ensures scalability and efficiency. Security mechanisms including multi-factor authentication, end-to-end encryption, and AI-based anomaly detection mitigate potential threats such as Sybil attacks and denial-of-service attacks. Comparative analysis indicates improved security, transparency, and cost-effectiveness over traditional systems. The proposed framework demonstrates strong technical feasibility and provides a foundation for future advancements in digital electoral systems.

Keywords: Blockchain, Electronic Voting, Distributed Ledger, Cryptography, PBFT, Smart Contracts.

I. INTRODUCTION

The increasing digitization of governance systems has highlighted the limitations of traditional voting mechanisms, including susceptibility to tampering, centralized control, and inefficiencies in vote counting. Ensuring transparency and trust in elections remains a critical challenge.

1.1 Problem Statement

Traditional voting systems face:

- Security vulnerabilities (tampering, cyberattacks)
- Lack of transparency in vote counting
- Limited accessibility for remote or disabled voters
- High operational costs and inefficiencies

1.2 Proposed Solution

To address these challenges, this paper proposes a blockchain-based voting system that:

- Eliminates central authority dependency
- Ensures immutability of votes
- Provides transparency through distributed ledgers
- Maintains voter anonymity using cryptographic techniques

1.3 Objectives

- Design a secure blockchain voting architecture
- Ensure voter privacy and vote integrity
- Evaluate feasibility and scalability
- Address legal and regulatory considerations

II. LITERATURE REVIEW

2.1 Introduction to Blockchain in Voting Systems

Blockchain technology has emerged as a transformative solution for secure digital transactions due to its decentralized, immutable, and transparent nature. In the context of voting systems,

blockchain eliminates the reliance on centralized authorities and ensures that once a vote is recorded, it cannot be altered or deleted. This makes it particularly suitable for electoral processes where trust and integrity are paramount. Blockchain is a distributed ledger system where transactions are recorded immutably across multiple nodes. Core components include:

- Cryptographic hashing
- Distributed consensus mechanisms
- Decentralized architecture

2.2 Evolution of Electronic Voting Systems

Electronic voting systems have evolved from basic Electronic Voting Machines (EVMs) to internet-based voting platforms. While EVMs improved efficiency, they remain vulnerable to tampering and lack transparency. Internet voting systems, although more accessible, introduce risks such as cyberattacks, data breaches, and identity theft.

Blockchain-based systems represent the next stage in this evolution by combining decentralization with cryptographic security, thereby addressing many of the shortcomings of previous systems.

Existing systems such as Voatz and Estonia's eVoting platform demonstrate feasibility but reveal limitations in scalability and security.

2.3 Analysis of Existing Blockchain Voting Systems

Several blockchain-based voting implementations have been proposed and tested:

- Voatz Platform: Enabled mobile-based voting but faced criticism for potential security vulnerabilities.
- Estonia eVoting System: Demonstrated large-scale feasibility but relies partially on centralized components.
- Follow My Vote: Focused on transparency but lacked scalability for national elections.

These systems highlight that while blockchain offers strong potential, challenges related to scalability, usability, and security still persist.

2.4 Cryptographic Techniques in Voting Systems

Security in blockchain voting systems is achieved through advanced cryptographic techniques:

- Elliptic Curve Cryptography (ECC): Provides secure key exchange with lower computational overhead.
- Zero-Knowledge Proofs (ZKPs): Allow verification of voter identity without revealing personal data.
- Homomorphic Encryption: Enables vote counting without decrypting votes.
- Hash Functions (SHA-256): Ensure data integrity and immutability.

These techniques collectively ensure confidentiality, integrity, and authentication within the system.

2.5 Consensus Mechanisms

Consensus protocols play a crucial role in validating transactions:

- Proof of Work (PoW): Highly secure but energy-intensive
- Proof of Stake (PoS): More efficient but may introduce centralization risks
- Practical Byzantine Fault Tolerance (PBFT): Suitable for permissioned networks with low latency

PBFT is particularly effective for voting systems as it ensures fast and reliable consensus among trusted nodes.

2.6 Challenges in Blockchain Voting

Despite its advantages, blockchain voting faces several challenges:

- Scalability Issues: Handling millions of votes simultaneously
- Security Risks: Smart contract vulnerabilities
- Legal Constraints: Lack of regulatory frameworks
- Digital Divide: Accessibility issues for non-technical users

2.7 Research Gap

Existing systems fail to provide a fully integrated solution that combines:

- High scalability
- Strong privacy mechanisms
- User-friendly interfaces
- Legal compliance

The proposed system aims to bridge these gaps through a hybrid architecture and enhanced security framework.

III. METHODOLOGY

3.1 Research Approach

This research follows a Design Science Research Methodology (DSRM), focusing on designing and evaluating a technological solution for secure voting.

3.2 System Architecture

The system is divided into three primary layers:

1. Application Layer

- User interface for voters and administrators
- Handles authentication and vote submission

2. Blockchain Layer

- Maintains distributed ledger
- Executes smart contracts
- Validates votes using PBFT consensus

3. Storage Layer

- On-chain storage for votes
- Off-chain storage (IPFS) for scalability

3.3 Workflow of the System

- Voter registration and verification
- Authentication using multi-factor methods
- Vote encryption
- Vote submission to blockchain
- Consensus validation
- Storage and tallying

3.4 Data Processing Techniques

- Data validation to prevent invalid inputs
- Encryption before transmission
- Duplicate vote detection
- Integrity verification using hashes

3.5 Security Implementation

- End-to-end encryption
- Role-Based Access Control (RBAC)
- Secure key management using HSM
- Continuous monitoring using AI

3.6 Advantages of Methodology

- High security and transparency
- Reduced human intervention
- Improved efficiency

3.7 Limitations

- Dependency on internet infrastructure
- Requires digital literacy
- Initial setup cost is high

IV. PROPOSED SYSTEM DESIGN

4.1 System Architecture Overview

The proposed system uses a three-tier architecture ensuring modularity and scalability.

4.2 Voter Authentication Process

- Registration through government databases

Multi-factor authentication:

- Biometrics
- OTP verification
- Cryptographic keys

4.3 Voting Process

- Vote is encrypted using SHA-256
- Signed using private key
- Broadcast to blockchain network
- Verified through consensus
- Stored permanently

4.4 Smart Contract Design

Smart contracts automate:

- Voter validation
- Vote recording
- Vote counting
- Result declaration

4.5 Privacy Mechanisms

- Separation of identity and vote

- Zero-Knowledge Proofs
- Anonymous transactions

4.6 Security Framework
Protection against:

- Sybil attacks
- DoS attacks
- Smart contract exploits

4.7 System Benefits

- Tamper-proof voting
- Real-time result processing
- Increased voter participation

V. RESULTS AND ANALYSIS

5.1 Expected Results
The system is expected to:

- Improve election security
- Increase transparency
- Reduce operational costs
- Enable remote voting

5.2 Performance Metrics

- Transaction throughput
- Latency in vote processing
- Accuracy of vote counting

5.3 Comparative Analysis

Feature	Traditional Voting	Blockchain Voting
Security	Low	High
Transparency	Limited	High
Cost	High	Moderate
Speed	Slow	Fast

5.4 Feasibility Analysis

- Technical Feasibility
- Mature blockchain platforms available
- Scalable infrastructure
- Economic Feasibility
- High initial cost
- Long-term savings
- Legal Feasibility
- Requires regulatory adaptation
- Supported by global pilot programs

VI. CONCLUSION AND FUTURE SCOPE

6.1 Conclusion
In this paper, a blockchain-based voting system was proposed to enhance the security, transparency, and efficiency of modern electoral processes. The system addresses critical limitations of traditional voting methods, including vulnerability to tampering, lack of transparency, and dependence on centralized authorities. By leveraging decentralized ledger technology, the proposed framework ensures that all votes are recorded immutably and can be verified without compromising voter privacy.

The architecture of the system, consisting of application, blockchain, and storage layers, enables a seamless flow of data from voter authentication to final result generation. This layered design improves system scalability, reliability, and overall performance. Features such as cryptographic vote encryption, smart contract-based automation, and consensus-driven validation contribute to a secure and efficient voting mechanism. Additionally, privacy-preserving techniques such as Zero-Knowledge Proofs ensure that voter anonymity is maintained while preserving auditability.

The proposed framework also incorporates robust security measures, including multi-factor authentication, encryption protocols, and protection against common cyber threats such as Sybil and denial-of-service attacks. Furthermore, the system aligns with legal and ethical considerations, making it suitable for deployment in real-world electoral environments where data protection and regulatory compliance are essential.

Overall, the blockchain-based voting system demonstrates the effectiveness of integrating decentralized technologies with advanced cryptographic techniques to modernize electoral systems. It reduces manual intervention, minimizes the risk of fraud, and enhances trust in the voting process. The system provides a practical and scalable

solution for future digital elections, addressing the growing need for secure and transparent governance in an increasingly digital world.

The proposed system successfully addresses the limitations of traditional voting methods and presents a scalable and secure alternative for modern elections.

6.2 Future Scope

Future enhancements may include:

- Integration of quantum-resistant cryptography
- Use of AI for fraud detection
- Implementation of real-time large-scale voting systems
- Development of global regulatory frameworks
- Integration with digital identity systems (e.g., Aadhaar-based verification)

REFERENCES

1. Hajian Berenjestanaki, M., et al., "Blockchain-Based E-Voting Systems: A Technology Review," Electronics (MDPI), vol. 13, no. 1, 2023.
2. Daraghmi, E., Hamoudi, A., & Abu Helou, M., "Secure and Transparent E-Voting Systems with Blockchain Technology," Future Internet, vol. 16, no. 11, 2024.
3. Sujatha, B., et al., "Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication and Election Automation," Indian Journal of Science and Technology, vol. 17, 2024.
4. Somasekhar, G., et al., "Digital Voting with Blockchain using IPFS for Secure Data Storage," Engineering, Technology & Applied Science Research, 2024.
5. Hyperledger Foundation, "Hyperledger Fabric Documentation," [Online]. Available: https://hyperledger-fabric.readthedocs.io/
6. Ethereum Foundation, "Ethereum Blockchain Platform," [Online]. Available: https://ethereum.org/
7. IPFS Team, "InterPlanetary File System (IPFS) Documentation," [Online]. Available: https://docs.ipfs.tech/
8. Revelo Sánchez, O., "Systematic Review of Blockchain-Based Electronic Voting Systems (2022–2025)," Technologies (MDPI), 2026.
9. "Blockchain-Enabled Smart Contract Voting Systems: Challenges and Opportunities," ScienceDirect, 2025.

Screenshots