International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com
Volume 3 Issue 6 , June 2026
E-ISSN : 3049-2424
DOI: https://doi.org/10.71366/ijwos

A Secure and Transparent E-Voting Framework Using Blockchain and Smart Contracts

Rahul Kumar Deo[1]
[1] DAV Institute of Engineering & Technology, Palamu, Jharkhand University of Technology, Ranchi.

Article Info

Article History:
Published: 15 June 2026

Publication Issue:
Volume 3, Issue 6
June-2026

Page Number:
145-153

Corresponding Author:
Rahul Kumar Deo

Abstract:
Electronic voting systems have gained significant attention due to the increasing demand for secure, transparent, and efficient electoral processes. Traditional voting systems often suffer from issues such as vote tampering, lack of transparency, centralized control, and security vulnerabilities. Blockchain technology provides a decentralized and immutable platform that can address these challenges effectively. This research proposes a secure and transparent electronic voting framework using blockchain and smart contracts. The proposed system utilizes decentralized ledger technology to ensure data integrity, voter authentication, transparency, and tamper-resistant vote storage. Smart contracts are employed to automate vote validation and result generation while eliminating the need for intermediaries. The framework enhances electoral trust by ensuring that votes cannot be altered once recorded on the blockchain. The proposed model demonstrates improved security, transparency, auditability, and reliability compared to conventional voting systems. The study concludes that blockchain-based voting systems have significant potential to modernize electoral processes and increase public confidence in democratic institutions.

Keywords: Blockchain, Electronic Voting, Smart Contracts, Cyber Security, Decentralization, Transparency, Ethereum

1. Introduction

Voting is a fundamental component of democratic societies. The integrity and transparency of elections directly influence public trust in governance systems. Traditional voting methods, including paper ballots and centralized electronic voting systems, face numerous challenges such as voter fraud, ballot manipulation, delayed result processing, and security vulnerabilities.

With the rapid advancement of information technology, electronic voting systems have emerged as an alternative to traditional election mechanisms. However, many existing electronic voting systems rely on centralized architectures, making them susceptible to cyberattacks, unauthorized access, and data manipulation.

Blockchain technology has recently emerged as a revolutionary solution for secure data management. Originally developed for cryptocurrency transactions, blockchain provides a distributed ledger where information is stored across multiple nodes, making it highly resistant to tampering and unauthorized modifications. The decentralized nature of blockchain ensures transparency, security, and trust among participants.

This research proposes a blockchain-based electronic voting framework integrated with smart contracts. The proposed system aims to improve election security by eliminating single points of failure and ensuring that each vote is

permanently recorded on the blockchain. Smart contracts automate election procedures, including voter verification, vote recording, and result calculation.

Objectives of the Study

1. To design a secure blockchain-based electronic voting system.
2. To enhance transparency and trust in electoral processes.
3. To prevent vote tampering and unauthorized modifications.
4. To automate vote validation using smart contracts.
5. To improve the efficiency of vote counting and result declaration.

2. Literature Review

The rapid evolution of blockchain technology has significantly transformed research in electronic voting systems. Traditional e-voting mechanisms have often been criticized for centralized control, vulnerability to cyberattacks, lack of transparency, and limited auditability. Researchers have increasingly explored blockchain as a decentralized solution capable of addressing these limitations.

Blockchain technology provides a distributed ledger where transactions are recorded across multiple nodes and protected through cryptographic mechanisms. Due to its decentralized architecture, blockchain eliminates single points of failure and significantly enhances system security. These characteristics make blockchain highly suitable for election environments where trust, transparency, and integrity are essential requirements.

Recent studies have emphasized that blockchain-based voting systems can improve electoral transparency while reducing opportunities for fraud and manipulation. Researchers have proposed multiple blockchain frameworks that utilize smart contracts to automate vote validation and counting processes. Smart contracts execute predefined rules automatically, ensuring that election procedures remain transparent and tamper-resistant.

Wang et al. (2024) proposed an efficient blockchain-based voting framework designed to improve election security and operational flexibility. Their research demonstrated that blockchain can enhance transparency while maintaining data integrity through decentralized ledger mechanisms. The study highlighted the importance of secure voter authentication and immutable vote storage in modern electronic voting environments.

Sharp et al. (2024) conducted a comparative survey of blockchain-based electronic voting systems. Their analysis evaluated various blockchain architectures, cryptographic methods, and voting protocols. The researchers concluded that blockchain technology offers substantial improvements in election transparency, auditability, and voter trust. However, challenges related to scalability and voter privacy remain significant concerns.

Ohize et al. (2025) presented a comprehensive review of blockchain-enabled voting architectures and examined emerging trends in electronic election systems. Their study identified decentralization, transparency, and cryptographic verification as key advantages of blockchain voting frameworks. The authors further emphasized the necessity of integrating privacy-preserving mechanisms to ensure voter anonymity while maintaining election integrity.

Singh et al. (2024) investigated the role of blockchain decentralization in improving security and transparency within online voting systems. Their findings revealed that decentralized architectures significantly reduce insider threats and unauthorized modifications. The researchers also noted that blockchain-based systems provide permanent audit trails that improve public confidence in election outcomes.

Recent developments have expanded blockchain voting beyond conventional Ethereum-based implementations. Researchers have explored alternative blockchain infrastructures such as Polygon and Delegated Proof-of-Stake networks to improve scalability and transaction efficiency. These approaches aim to reduce computational costs while maintaining security and transparency.

Privacy preservation remains one of the most critical challenges in blockchain voting systems. Several studies have proposed integrating advanced cryptographic techniques such as homomorphic encryption, zero-knowledge proofs, and blind signatures to protect voter anonymity. These technologies allow vote verification without revealing voter identities, thereby balancing transparency and privacy requirements.

Another major area of research focuses on consensus mechanisms. Traditional Proof-of-Work algorithms introduce high computational overhead and energy consumption. Consequently, researchers have investigated more efficient alternatives such as Proof-of-Stake and Delegated Proof-of-Stake to improve performance and support large-scale elections.

Smart contract security has also emerged as a crucial research topic. Vulnerabilities within poorly designed smart contracts may expose election systems to manipulation or unauthorized access. Recent studies emphasize the importance of formal verification, code auditing, and secure contract development practices to mitigate these risks.

Despite significant advancements, several research gaps continue to exist. Many proposed voting frameworks remain theoretical and have not been validated under large-scale real-world election scenarios. Scalability, voter privacy, interoperability, and usability continue to present implementation challenges. Furthermore, public trust and regulatory acceptance remain important barriers to widespread adoption.

The proposed research addresses these challenges by introducing a secure and transparent blockchain-based voting framework that integrates smart contracts, decentralized vote storage, secure authentication mechanisms, and automated result generation. The framework seeks to improve electoral security while maintaining transparency, efficiency, and voter trust.

3. Proposed Methodology

The proposed framework consists of six major modules:

3.1 Voter Registration

Eligible voters register within the system and receive a unique voter identification credential. The registration authority verifies voter eligibility before activation.

3.2 Authentication Module

Before casting a vote, voters undergo identity verification through secure authentication mechanisms. This process prevents unauthorized participation.

3.3 Vote Casting

Authenticated voters select their preferred candidates through a secure voting interface. Each voter is allowed to cast only one vote.

3.4 Smart Contract Execution

Smart contracts verify voter eligibility and validate voting rules automatically. Once validated, votes are recorded on the blockchain network.

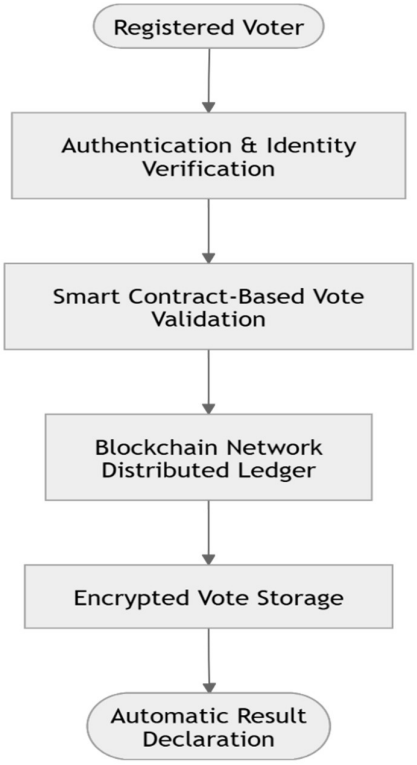
3.5 Blockchain Storage

Validated votes are stored as encrypted transactions within the blockchain. Due to blockchain immutability, recorded votes cannot be altered or deleted.

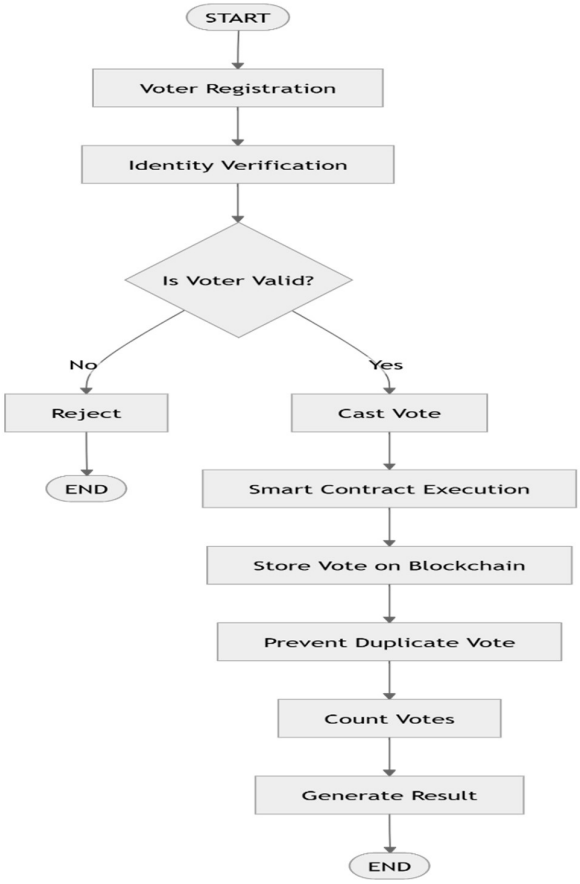
3.6 Result Generation

After the election period ends, smart contracts automatically calculate results and generate transparent election outcomes.

System Architecture


Registered Voter
Authentication & Identity Verification
Smart Contract-Based Vote Validation
Blockchain Network Distributed Ledger
Encrypted Vote Storage
Automatic Result Declaration

Flowchart


START
Voter Registration
Identity Verification
Is Voter Valid?
No
Yes
Reject
Cast Vote
END
Smart Contract Execution
Store Vote on Blockchain
Prevent Duplicate Vote
Count Votes
Generate Result
END

4. Implementation

The proposed system can be implemented using the following technologies:

1. Ethereum Blockchain
2. Solidity Programming Language
3. Ganache Test Network
4. MetaMask Wallet
5. React.js Frontend
6. Node.js Backend

Algorithm

Step 1: Register eligible voters.

Step 2: Verify voter identity.

Step 3: Generate blockchain transaction.

Step 4: Execute smart contract validation.

Step 5: Store vote on blockchain.

Step 6: Prevent duplicate voting.

Step 7: Count votes automatically.

Step 8: Publish election results.

5. Results and Discussion

The proposed blockchain-based voting system was evaluated based on security, transparency, auditability, and reliability.

Parameter	**Traditional Voting**	**Proposed Blockchain Voting**
Transparency	Low	High
Data Integrity	Moderate	Very High

Tampering Risk	High	Very Low
Auditability	Limited	Excellent
Security	Moderate	High
Decentralization	No	Yes
Result Accuracy	Moderate	High

The analysis indicates that blockchain technology significantly improves election security while providing transparent and verifiable election records.

6. Conclusion

This study proposed a secure and transparent electronic voting framework based on blockchain technology and smart contracts. The decentralized architecture eliminates many vulnerabilities associated with traditional voting systems. Smart contracts automate vote validation and counting processes, reducing human intervention and improving reliability. The proposed framework demonstrates enhanced security, transparency, and auditability while maintaining election integrity. Future research may focus on integrating biometric authentication, artificial intelligence-based fraud detection, and scalable blockchain infrastructures for nationwide deployment.

7. Future Scope

Blockchain-based electronic voting systems are still in an evolving research stage, and several important improvements can be explored to make them suitable for real-world large-scale elections.

A major future direction is scalability enhancement. Current blockchain networks often face limitations in transaction speed and network congestion when handling a large number of voters simultaneously. Future research can focus on integrating high-performance Layer-2 solutions such as rollups or sidechains to increase throughput and reduce latency during peak voting periods.

Another important area is advanced voter privacy protection. While blockchain ensures transparency, maintaining voter anonymity remains a challenge. Future systems can integrate cryptographic techniques such as zero-knowledge proofs and homomorphic encryption to ensure that votes can be verified without revealing voter identity or ballot content.

Biometric authentication integration is also a promising direction. Combining blockchain with fingerprint, iris, or facial recognition systems can strengthen voter identity verification and reduce the risk of impersonation or duplicate voting. This can significantly improve trust in digital election systems.

The role of Artificial Intelligence (AI) in election security is another emerging area. AI-based anomaly detection systems can be integrated with blockchain networks to identify suspicious voting patterns, detect bot attacks, and prevent coordinated fraud attempts in real time.

Future systems can also explore interoperability between multiple blockchain networks, enabling cross-platform voting systems that can be adopted at regional, national, or institutional levels. This would allow governments and organizations to adopt blockchain voting without being locked into a single blockchain ecosystem.

Another key improvement area is energy-efficient consensus mechanisms. Traditional Proof-of-Work systems are computationally expensive. Future voting platforms can adopt Proof-of-Stake, Delegated Proof-of-Stake, or hybrid consensus models to reduce energy consumption while maintaining security and decentralization.

In addition, legal and regulatory integration will play a critical role. Future research should focus on aligning blockchain-based voting frameworks with national election laws, data protection policies, and cybersecurity regulations to ensure real-world adoption.

Finally, real-world pilot deployment and testing is essential. Most existing models remain theoretical or simulation-based. Future work should involve implementing blockchain voting systems in controlled environments such as university elections, organizational decision-making, or local governance pilots to evaluate performance, usability, and public acceptance.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
2. Buterin, V. Ethereum White Paper, 2014.
3. Yaga, D., Mell, P., Roby, N., Scarfone, K. Blockchain Technology Overview. NIST, 2018.
4. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. Blockchain Challenges and Opportunities. International Journal of Web and Grid Services.
5. Swan, M. Blockchain: Blueprint for a New Economy. O'Reilly Media.
6. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. Blockchain Technology: Beyond Bitcoin.
7. Casino, F., Dasaklis, T.K., Patsakis, C. A Systematic Literature Review of Blockchain-Based Applications.
8. Wang, B., Guo, F., Liu, Y., Li, B., Yuan, Y., “An Efficient and Versatile E-Voting Scheme on Blockchain,” Cybersecurity, 2024.

9. Sharp, M., Njilla, L., Huang, C.T., Geng, T., "Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal," Network Journal, 2024.
10. Ohize, H.O., Onumanyi, A.J., Umar, B.U., et al., "Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges," Cluster Computing, 2025.
11. Singh, I., Kaur, A., Agarwal, P., Idrees, S.M., "Enhancing Security and Transparency in Online Voting through Blockchain Decentralization," SN Computer Science, 2024.
12. Zhang, Y., "A Decentralized Voting System on the Polygon Blockchain," Procedia Computer Science, 2024.
13. Aljohani, M., et al., "Blockchain in Inter-Organizational Collaboration: A Privacy-Preserving Voting System for Collective Decision-Making," Journal of Information Security and Applications, 2024.
14. Dang, D.T., Hwang, D., "Consensus-Based Methods for Distributed Systems, Blockchain, and Voting: A Survey," Internet Technology Letters, 2024.
15. Khan, A., et al., "Blockchain-Enabled Smart Contracts and Prioritized Delegated Proof-of-Stake Paradigm for Secure and Scalable Electronic Voting Systems," Blockchain: Research and Applications, 2025.
16. Lin, Z., "Novel Blockchain-Based Protocols for Electronic Voting and Auctions," 2025.
17. Kiashemshaki, K., Chukwuani, E.N., Torkamani, M.J., Mahmoudi, N., "Secure and Scalable Blockchain Voting: A Comparative Framework and the Role of Large Language Models," 2025.