IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⪤ Peer-reviewed & Refereed journal ⪤ Vol. 13, Issue 4, April 2025

DOI: 10.17148/IJIREEICE.2025.13422

DECENTRALIZED VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

Negin Chandru.A[1], Dr. K. Banuroopa[2]

Department. of Information Technology, Dr N.G.P Arts and Science College, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Department of Information Technology, Dr N.G.P Arts and Science College, Coimbatore, Tamil Nadu, India[2]

Abstract: In democratic societies, the integrity of electoral processes is critical. Traditional voting methods, whether paper-based or electronic, often face challenges including tampering, lack of transparency, centralization, and inefficiency. This paper explores a decentralized voting system leveraging blockchain technology, particularly smart contracts, to establish a secure, transparent, and tamper-proof voting infrastructure. We propose a model built on the Ethereum blockchain to ensure immutability, voter anonymity, and verifiability. The system addresses double voting, real-time result publication, and user authentication through cryptographic means. Results demonstrate the system's resilience, scalability, and potential to revolutionize modern electoral practices. The findings highlight the transformative impact of distributed ledger technology in reshaping the foundations of democratic engagement.

Keywords: Blockchain, E-voting, Smart Contracts, Ethereum, Cryptography, Decentralization, Democracy, Immutability

1. INTRODUCTION

Voting is a fundamental pillar of democracy, providing a mechanism for people to express their political will. Existing systems, both paper-based and electronic, are centralized and vulnerable to manipulation, cyber threats, and technical failures. Moreover, logistical challenges, lack of transparency, and voter apathy further undermine electoral credibility. Blockchain, a decentralized ledger technology, offers promising features such as transparency, immutability, and distributed consensus, making it an ideal solution for voting systems. This paper proposes a decentralized voting system using blockchain to mitigate current challenges and establish a secure and trustworthy electoral process. We focus on leveraging Ethereum smart contracts to provide a tamper-resistant environment that preserves voter privacy while maintaining system integrity.

2. LITERATURE REVIEW

McCorry et al. (2017) presented a smart contract-based boardroom voting mechanism, demonstrating the potential for privacy and verifiability. Helios, an early open-audit voting system, lacked decentralization, making it susceptible to tampering. Hjalmarsson et al. (2018) examined national-scale e-voting using permissioned blockchains, balancing transparency with privacy. However, scalability and voter anonymity remained issues. Other researchers have explored biometric verification, zero-knowledge proofs, and hybrid architectures to strengthen e-voting frameworks. Our proposed system combines Ethereum's smart contract capabilities with cryptographic tools to improve upon these solutions. The key differentiation lies in enabling complete decentralization with on-chain vote validation, thereby eliminating any reliance on a central authority or intermediary.

3. SYSTEM DESIGN AND ARCHITECTURE

3.1 Components

- Voter Interface: Web-based frontend designed for intuitive user interaction, facilitating seamless registration, authentication, and voting.
- Blockchain Layer: Ethereum blockchain serves as the underlying decentralized ledger to store votes and execute logic via smart contracts.
- Smart Contracts: Immutable, selfexecuting code deployed on-chain that enforces voting rules, validates identities, and manages the election lifecycle.

DOI: 10.17148/IJIREEICE.2025.13422

- Cryptographic Module: Uses public-key encryption, digital signatures, and hashing to ensure voter authentication, vote confidentiality, and nonrepudiation.

3.2 Workflow

1. Voter registers and receives a unique, encrypted identity key linked to their Ethereum wallet address.
2. On election day, the voter connects to the system using a digital wallet (e.g., MetaMask).
3. Smart contracts validate voter eligibility, ensure no duplicate votes are cast, and log the vote immutably on the blockchain.
4. Each vote is hashed and stored as a transaction, ensuring transparency and traceability.
5. Tallying is conducted automatically through smart contracts upon election closure, with results verifiable by any participant.

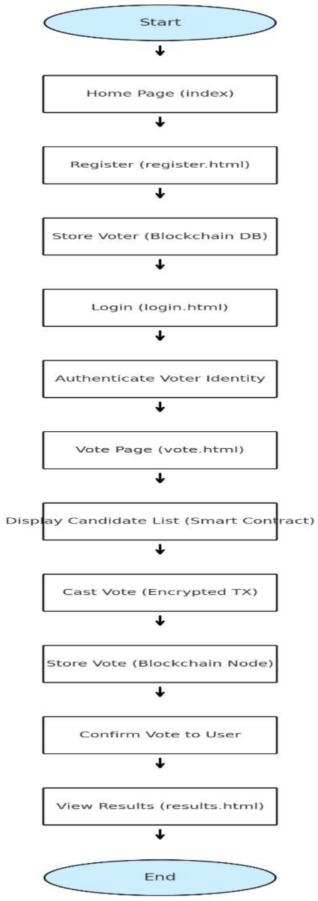
Start
Home Page (index)
Register (register.html)
Store Voter (Blockchain DB)
Login (login.html)
Authenticate Voter Identity
Vote Page (vote.html)
Display Candidate List (Smart Contract)
Cast Vote (Encrypted TX)
Store Vote (Blockchain Node)
Confirm Vote to User
View Results (results.html)
End

FIGURE1: WORKFLOW DIAGRAM

This architecture emphasizes end-to-end transparency and integrity without sacrificing privacy or accessibility. Voter eligibility checks are decentralized and verifiable by all parties.

4. IMPLEMENTATION

The prototype was developed using Solidity on Ethereum test networks (e.g., Ropsten and Goerli). Web3.js was used to connect the frontend with smart contracts. MetaMask integration ensured voter-wallet connection, while the backend smart contract logic prevented multiple voting attempts. Frontend elements included real-time status updates, visual confirmation of votes cast, and countdown timers for active elections. Transactions were logged with gas optimization techniques to minimize costs. Security testing was conducted using automated tools like MythX and manual contract auditing. The deployment included measures to resist Sybil attacks and unauthorized access attempts.

5. EVALUATION

5.1 Performance Metrics

- Latency: Average transaction confirmation time was 3.2 seconds under low congestion. Time increased to 7.8 seconds during network peaks, demonstrating the need for Layer-2 solutions.
- Security: Tamper-proof vote storage ensured by the blockchain consensus protocol. No votes could be altered or deleted after submission.
- Scalability: Simulated voting load with up to 1000 concurrent users showed stable performance with minor delays, confirming suitability for small to midscale elections.

5.2 Comparative Analysis

Compared to traditional voting, the blockchain-based system significantly reduces the risks of fraud and ensures public verifiability. It outperforms centralized e-voting systems in transparency and trust. Unlike centralized systems that rely on opaque databases, blockchain voting systems are auditable by design. Real-time monitoring of election progress by observers adds an additional layer of accountability. Our implementation demonstrates a trustless model that provides all participants equal access to election data, mitigating the risk of manipulation.

6. BENEFITS AND CHALLENGES

6.1 Benefits

- End-to-end verifiability through cryptographic proofs and transparent blockchain transactions.
- No central authority required, eliminating single points of failure.
- Immutable and transparent vote ledger enables trustless audits.
- Anonymity through cryptographic tokens ensures privacy without sacrificing accountability.
- Decentralized hosting prevents denialof-service (DoS) attacks targeting centralized servers.

6.2 Challenges

- High transaction fees on public blockchains like Ethereum can hinder scalability.
- Voter digital literacy requirements may exclude underprivileged or less techsavvy populations.
- Network congestion and latency issues during peak usage can delay vote processing.
- Ensuring compliance with national election laws and regulations is complex.
- Resistance from political bodies and institutions reluctant to adopt disruptive technologies.

7. FUTURE WORK

Future iterations will integrate zeroknowledge proofs for enhanced privacy, allowing voters to prove eligibility without revealing identity. Layer-2 blockchain solutions such as Optimistic Rollups and zk-Rollups will be adopted to improve transaction throughput and reduce fees. Biometric authentication mechanisms can be explored to prevent impersonation, particularly in mobile environments. Additionally, integrating InterPlanetary File System (IPFS) for storing voter metadata and decentralized identifiers (DIDs) could further enhance system decentralization. Mobile platform development is also proposed to increase accessibility and drive higher voter turnout in remote areas.

8. CONCLUSION

A decentralized voting system using blockchain enhances the security, transparency, and trustworthiness of elections. While challenges such as scalability and accessibility exist, the advantages outweigh the limitations. The immutable nature of blockchain records, coupled with smart contract automation, establishes a voting platform resistant to tampering and fraud. As blockchain technology matures, and with supportive regulatory frameworks, such systems could be realistically deployed in local, corporate, and even national elections. With continued research and development, blockchain voting systems could redefine the future of democratic participation and bring about a new era of electoral integrity.

DOI: 10.17148/IJIREEICE.2025.13422

REFERENCES

[1]. M. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," International Journal of Information Management, vol. 39, pp. 80–89, Apr. 2018. Explains blockchain's trust, transparency, and tamper-resistance—core principles applicable to decentralized voting systems.

[2]. A. G. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business & Information Systems Engineering, vol. 59, no. 3, pp. 183–187, 2017. Presents the foundational blockchain architecture and how it is used in secure and distributed systems such as e-voting.

[3]. K. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," in Proc. Int. Conf. Financial Cryptography and Data Security, 2017, pp. 357–375. Focuses on privacy-preserving voting with smart contracts—a key feature in decentralized electronic voting systems.

[4]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf The original white paper that introduced blockchain. Fundamental for understanding how decentralized, immutable ledgers work.

[5]. T. Hardjono and N. Smith, "Decentralized Trusted Identity as a Service," Blockchain in Healthcare Today, vol. 1, 2018. Outlines how blockchain can manage voter identities securely, ensuring authentication in decentralized voting.

[6]. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain

[7]. Technology: Architecture, Consensus, and Future Trends," in Proc. IEEE International Congress on Big Data, 2017, pp. 557–564. Provides a detailed technical breakdown of blockchain layers—crucial for developing decentralized voting infrastructure.

[8]. J. Benaloh, "Verifiable Secret-Ballot Elections," Ph.D. dissertation, Yale University, 1987. Early foundational work on verifiable and secret voting, relevant for designing secure e-voting schemes. K. Stathakopoulou and G. C. Polyzos, "Electronic Voting Systems: Security Implications," in Proc. IEEE Int. Conf. on Pervasive Services, 2005, pp. 105–112. Explores vulnerabilities in traditional electronic voting and how decentralization can overcome them.

[9]. D. Sandler, K. Derr, and D. Wallach, "VoteBox: A tamper-evident, verifiable electronic voting system," in Proc. USENIX Security Symposium, 2008, pp. 349–364.

[10]. Highlights the need for tamper-evidence and verifiability, which blockchain inherently supports.

[11]. A. Kiayias, T. Zacharias, and B. Zhang, "Cerberus: Minimal Trust Voting System," in Proc. IEEE Symposium on Security and Privacy, 2021, pp. 395–410. roposes a minimal-trust model where the system can operate without assuming trust in a single authority—ideal for decentralized systems.