© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715963

A Comprehensive Study of Blockchain-Based E-Voting Systems: Architecture, Security, and Challenges

SANJU S[1], RACHANA H[2], V NAVITHA[3]
[1, 2, 3] *Dept. of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, Bangalore*

Abstract - Electronic voting (e-voting) systems aim to modernize electoral processes by making them more efficient, accessible, and reliable. However, traditional methods face challenges like lack of transparency, vulnerability to tampering, and dependence on centralized authorities. Blockchain technology offers a promising solution by providing a decentralized, unchangeable, and transparent way to securely record and verify votes. This paper surveys blockchain-based e-voting systems by reviewing ten research studies. It focuses on their methods, including system designs, consensus mechanisms like Proof of Work and Practical Byzantine Fault Tolerance, and cryptographic techniques such as digital signatures and ring signatures. The study emphasizes the benefits of blockchain, including improved security, auditability, and trust. It also points out major challenges like scalability, privacy concerns, voter authentication, and regulatory issues. The findings show that while blockchain has great potential to change e-voting systems, more research is needed to create scalable, privacy-protecting, and practical solutions for real-world use.

Index Terms - Blockchain, Electronic voting, Security, Smart contracts, Transparency

I. INTRODUCTION

Electronic voting (e-voting) has become a key way to modernize elections by using digital technologies to improve efficiency, accessibility, and speed. Traditional voting systems, whether paper-based or electronic voting machines (EVMs), often encounter issues like a lack of transparency, risks of tampering, slow result processing, and low voter trust. These problems have led researchers to look for more secure, transparent, and tamper-resistant options.

To address these issues, researchers are looking into new technologies to improve the security, transparency, and reliability of digital voting systems beyond what traditional methods offer.

In recent years, blockchain technology has gained significant attention as a promising solution to address the inherent issues in conventional e-voting systems. Blockchain is a decentralized and distributed ledger technology that ensures data integrity, immutability, and transparency through cryptographic mechanisms and consensus protocols. By eliminating the need for a central authority and enabling verifiable transactions, blockchain introduces a new paradigm for secure and trustworthy digital voting.

A blockchain-based e-voting system allows votes to be recorded as transactions in a distributed ledger, where each vote is encrypted, time-stamped, and linked to previous records, making unauthorized modifications virtually impossible. Furthermore, advanced cryptographic techniques such as digital signatures, zero-knowledge proofs, and ring signatures can be integrated to ensure voter anonymity while maintaining verifiability. Smart contracts also play a crucial role in automating the voting process, including voter authentication, ballot casting, and result tallying.

Despite these advantages, blockchain-based e-voting systems are not without challenges. Issues such as scalability, voter privacy, coercion resistance, computational overhead, and regulatory acceptance remain significant barriers to real-world deployment. Additionally, different research works propose varying architectures, consensus mechanisms, and security models, making it essential to systematically analyze and compare these approaches.

This survey paper aims to provide a comprehensive review of blockchain-based e-voting systems by examining key research contributions in the field. It focuses on understanding the methodologies adopted in existing works, evaluating their strengths and limitations, and identifying open challenges for future research. Through this study, the paper seeks to highlight how blockchain can reshape electoral systems while also addressing the practical concerns associated with its implementation.

II. RELATED WORK

Blockchain-based e-voting has attracted significant research attention in recent years, with numerous studies proposing frameworks, surveys, and implementation models to improve the security, transparency, and reliability of electoral systems.

Several survey papers provide a foundational understanding of this domain. Yedhukrishnan V et al. [1] present a comprehensive overview of blockchain-based e-voting systems, highlighting key architectural designs, consensus mechanisms, and security challenges. Similarly, Rabia Fatih et al. [2] conduct a comparative analysis of various blockchain voting models, emphasizing differences in scalability, privacy preservation, and system efficiency. Earlier work by Abuidris et al. [3] lays the groundwork by discussing fundamental principles of blockchain integration in voting systems and identifying core requirements such as anonymity, verifiability, and integrity. More recently, Dhruthana S et al. [6] extend these discussions by incorporating modern advancements such as Practical Byzantine Fault Tolerance (PBFT) and smart contract-based voting processes.

In addition to surveys, several researchers have proposed practical implementations of blockchain-based voting systems. Pavan M et al. [4] introduce a blockchain-enabled e-voting framework that leverages decentralized ledgers to ensure vote immutability and transparency. Similarly, Pathak et al. [5] design a system focused on enhancing electoral trust by preventing vote manipulation and ensuring secure voter authentication. Jaiswal et al. [7] emphasize the role of decentralization in eliminating single points of failure, proposing a system architecture that distributes control across multiple nodes.

Other studies focus on addressing specific challenges in e-voting. Sheikh et al. [8] highlight vulnerabilities in traditional electronic voting systems, such as EVM tampering and electoral fraud, and propose blockchain as a solution to mitigate these risks. A framework proposed by R. AlAbri et al. [9] provides a structured design approach, integrating security layers and system components to ensure robustness and scalability.

Advanced cryptographic techniques have also been explored to enhance privacy and security. Russo et al. [10], in their work “Chirotonia,” propose a scalable e-voting framework that combines blockchain technology with linkable ring signatures to ensure voter anonymity while maintaining auditability. This approach represents a significant step toward achieving both privacy preservation and transparency in decentralized voting systems.

Overall, the existing literature demonstrates a strong consensus on the potential of blockchain to revolutionize e-voting. While survey papers provide a broad understanding of the field, implementation-focused studies contribute practical solutions, and cryptographic approaches address critical security concerns. However, differences in design choices, consensus algorithms, and privacy mechanisms indicate the need for a detailed methodological comparison, which is discussed in the following section.

III. METHODOLOGY

The selected research papers propose a variety of methodologies for implementing blockchain-based e-voting systems. While all approaches leverage the core properties of blockchain - decentralization, immutability, and transparency - they differ in terms of system architecture, consensus mechanisms, cryptographic techniques, and implementation strategies.

3.1 System Architecture

Most of the proposed systems follow a three-layered architecture, consisting of:

- User Layer: Includes voters and election authorities who interact with the system through web or mobile interfaces.
- Application Layer: Handles voter authentication, ballot generation, and vote casting.
- Blockchain Layer: Stores votes as immutable transactions and ensures data integrity.

For instance, Pavan M et al. [4] and Jaiswal et al. [7] adopt a decentralized architecture where each vote is treated as a transaction and recorded on a distributed ledger. Similarly, the framework proposed by R. AlAbri et al. [9] introduces a modular architecture that separates authentication, voting, and result computation for better scalability and maintainability.

3.2 Consensus Mechanisms

Consensus algorithms play a crucial role in validating transactions and maintaining consistency across the network. The reviewed papers utilize different consensus protocols:

- Proof of Work (PoW): Used in some early models but criticized for high computational cost and latency.
- Proof of Stake (PoS): Offers improved efficiency and reduced energy consumption.
- Practical Byzantine Fault Tolerance (PBFT): Highlighted in Dhruthana S et al. [6], this method is widely preferred for permissioned blockchain systems due to its low latency and high throughput.

Most modern e-voting systems favor permissioned blockchains with PBFT or similar consensus mechanisms, as they provide faster transaction processing and controlled access, which is suitable for governmental elections.

3.3 Cryptographic Techniques

Security and privacy are central to e-voting systems, and various cryptographic methods are employed:

- Public-Key Cryptography: Ensures secure vote transmission and voter authentication.
- Digital Signatures: Used to verify voter identity and prevent impersonation.
- Hash Functions: Maintain data integrity by linking blocks securely.
- Ring Signatures: Used in "Chirotonia" (Russo et al., [10]) to provide anonymity while allowing vote verification.
- Zero-Knowledge Proofs (ZKP) (in some surveyed works): Enable validation of votes without revealing voter identity.

These techniques collectively ensure confidentiality, integrity, authentication, and non-repudiation.

3.4 Smart Contracts

Smart contracts are a key component in many proposed systems, automating critical processes such as:

- Voter registration and authentication
- Ballot issuance
- Vote casting
- Vote tallying and result declaration

Pathak et al. [5] and Sheikh et al. [8] emphasize the use of Ethereum-based smart contracts to eliminate human intervention and reduce the possibility of manipulation. Smart contracts ensure that once deployed, the voting logic cannot be altered, thereby enhancing trust.

3.5 Voter Authentication Mechanisms

Different approaches are used to authenticate voters before allowing them to cast votes:

- Biometric Authentication (fingerprint, facial recognition)
- Government-issued ID verification
- Multi-factor authentication (MFA)

Most systems integrate authentication with blockchain to ensure that only eligible voters participate, while also preventing duplicate voting.

3.6 Vote Storage and Tallying

Votes are typically:

- Encrypted before being cast
- Stored as transactions in the blockchain
- Linked using cryptographic hashes

For tallying:

Some systems use on-chain tallying, where results are computed directly from blockchain data.
Others use off-chain tallying to improve efficiency while maintaining verifiability.

Russo et al. [10] propose a scalable approach where vote verification and counting are optimized using cryptographic primitives, reducing computational overhead.

3.7 Security Mechanisms

To address common threats, the methodologies incorporate:

- Immutability to prevent vote tampering
- Decentralization to eliminate single points of failure
- Auditability to allow independent verification of results
- Anonymity mechanisms to protect voter identity

Sheikh et al. [8] and Pathak et al. [5] particularly focus on mitigating risks such as EVM hacking, insider attacks, and vote duplication.

Summary

Across the surveyed papers, the methodologies converge on a common goal: building a secure, transparent, and decentralized voting system. However, they differ in their choice of consensus algorithms, cryptographic techniques, and system designs. Table I provides a comparative summary of these approaches, highlighting variations in consensus mechanisms, security features, and system limitations.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1715963

TABLE I
COMPARISON OF BLOCKCHAIN BASED E-VOTING SYSTEMS

Ref	Year	Methodology	Consensus	Security Features	Advantages	Limitations
[1]	2024	Survey	N/A	Analysis-based	Comprehensive overview	No implementation
[2]	2023	Comparative Study	PoS/PBFT	Privacy + scalability	Detailed comparison	Limited real-world testing
[3]	2019	Survey	PoW	Basic security	Foundational concepts	Outdated methods
[4]	2023	Framework	PoS	Encryption, hashing	High transparency	Scalability issues
[5]	2021	Survey	Ethereum	Digital signatures	Automation	Contract vulnerabilities
[6]	2025	Survey + PBFT	PBFT	High fault tolerance	Efficient consensus	Partial centralization
[7]	2021	Decentralized model	PoW/PoS	Distributed control	No single failure	High cost
[8]	2022	Security-focused	PoS	Anti-tampering	Fraud prevention	Depends on external auth
[9]	2022	Structured framework	PBFT	Layered security	Scalable design	Complexity
[10]	2021	Cryptographic model	Custom	Ring signatures	Strong anonymity	High computation

IV. DISCUSSION

The analysis of the selected papers reveals that blockchain technology offers a strong foundation for building secure and transparent e-voting systems. However, despite significant progress, several trade-offs and unresolved challenges remain.

One of the most prominent advantages observed across all studies is enhanced security and data integrity. The use of cryptographic hashing and decentralized ledgers ensures that once a vote is recorded, it cannot be altered without detection. This effectively addresses major concerns associated with traditional voting systems, such as tampering and unauthorized modifications. Additionally, the transparency offered by blockchain enables public auditability, which can significantly increase voter trust in the electoral process.

Another key strength is decentralization, which eliminates the reliance on a central authority. Systems proposed by Pavan M et al. [4] and Jaiswal et al. [7] demonstrate how distributing control across multiple nodes reduces the risk of single points of failure and insider attacks. This is particularly important in large-scale elections where trust in centralized institutions may be limited.

However, the discussion also highlights important limitations and challenges.

A major issue is scalability. Public blockchain systems, especially those using Proof of Work, struggle to handle the high transaction throughput required for national elections. Even though permissioned blockchains and PBFT improve performance, they introduce partial centralization, which may compromise the core principle of decentralization.

Another critical concern is voter privacy and anonymity. While blockchain ensures transparency, it can conflict with the requirement of secret ballots. Advanced techniques like ring signatures (Russo et al [10]) and zero-knowledge proofs attempt to address this issue, but they often increase system complexity and computational overhead. Achieving a balance between transparency and privacy remains an open research problem.

Voter authentication is also a challenging aspect. Many proposed systems rely on external mechanisms such as biometric verification or government-issued IDs. While these improve security, they introduce dependencies on centralized systems, which contradict the decentralized philosophy of blockchain. Moreover, biometric systems raise concerns about data privacy and misuse.

The issue of coercion resistance is largely underexplored in the reviewed papers. In remote voting scenarios, voters may be influenced or forced to vote in a certain way, and blockchain alone cannot prevent this. This represents a significant gap between theoretical models and real-world deployment.

Additionally, usability and accessibility are often overlooked. Most systems focus heavily on technical robustness but fail to address whether the average voter can easily use the system. For large-scale adoption, user-friendly interfaces and minimal technical complexity are essential.

From an implementation perspective, smart contracts introduce both benefits and risks. While they automate the voting process and eliminate human intervention, any vulnerability in the contract code can lead to irreversible consequences. Since smart contracts are immutable after deployment, errors can be difficult to fix.

Finally, legal and regulatory challenges pose a major barrier to adoption. Electoral systems are highly sensitive and governed by strict regulations. Integrating blockchain into national voting infrastructure would require significant legal reforms, standardization, and government acceptance.

Overall Insight

The reviewed literature clearly demonstrates that blockchain has the potential to revolutionize e-voting systems by improving security, transparency, and trust. However, no single solution fully addresses all challenges. There is an inherent trade-off between decentralization, scalability, privacy, and usability, and future research must focus on achieving an optimal balance among these factors.

V. CONCLUSION

Blockchain-based e-voting systems represent a significant advancement in the evolution of digital electoral processes. This survey has examined various research contributions that leverage blockchain technology to address the limitations of traditional voting systems, such as lack of transparency, susceptibility to tampering, and dependence on centralized authorities.

From the reviewed literature, it is evident that blockchain provides key advantages including immutability, transparency, decentralization, and auditability, which collectively enhance the integrity and trustworthiness of voting systems. The integration of cryptographic techniques such as digital signatures, hashing, and ring signatures further strengthens security while attempting to preserve voter anonymity. Additionally, the use of smart contracts enables automation of the voting process, reducing human intervention and the risk of manipulation.

However, despite these benefits, several challenges hinder the widespread adoption of blockchain-based e-voting. Issues related to scalability, voter privacy, coercion resistance, usability, and regulatory compliance remain unresolved. The trade-offs between transparency and anonymity, as well as decentralization and performance, highlight the complexity of designing an ideal system. Furthermore, reliance on external authentication mechanisms and the risks associated with smart contract vulnerabilities present additional concerns.

Overall, while blockchain demonstrates strong potential to transform e-voting systems, it is not a complete solution in its current form. Future research should focus on developing scalable consensus mechanisms, privacy-preserving protocols, robust

authentication systems, and user-friendly interfaces, along with addressing legal and regulatory challenges. A hybrid approach that combines blockchain with other emerging technologies may offer a more practical and deployable solution for real-world elections.

VI. REFERENCES

[1] Yedhukrishnan V et al., "A Survey on E-Voting Systems Using Blockchain," IJERA, 2024.

[2] Rabia Fatih et al., "A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings," iJIM, 2023.

[3] Yousif Osman Abuidris et al., "A Survey of Blockchain-Based E-Voting Systems," ICBTA, 2019.

[4] Pavan M et al., "Blockchain Enabled E-Voting System," IJERT, 2023.

[5] Mrunal Pathak et al., "A Review on Blockchain Based E-Voting System," IJSRST, 2021.

[6] Dhruthana S et al., "Blockchain-Based E-Voting System – Literature Survey," IJCT, 2025.

[7] Shivam Jaiswal et al., "E-Voting Using Blockchain," IJERT, 2021.

[8] Mosin Sheikh et al., "Blockchain Based E-Voting System," IJRTI, 2022.

[9] R. AlAbri et al., "Designing an E-Voting Framework Using Blockchain Technology," International Journal of Electronic Government Research, 2022.

[10] Antonio Russo et al., "Chirotonia: A Scalable and Secure E-Voting Framework Based on Blockchains and Linkable Ring Signatures," arXiv, 2021.