Advanced International Journal for Research (AIJFR)
E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Review On Securing Elections for Digital Voting System with Blockchain Technology

Dimpal Kolhe[1], Dr. Himanshu V. Taiwade[2]

[1]Research Scholar, Department of Computer Science & Engineering, Priyadarshini College of Engineering, Nagpur, India
[2]Assistant Professor, Department of Computer Science & Engineering, Priyadarshini College of Engineering, Nagpur, India

Abstract

Vote manipulation, fraud, inefficiency, and a lack of transparency are just a few of the major issues facing traditional voting methods that erode public confidence in democratic processes. In order to improve election security, transparency, and efficiency, this study suggests a blockchain networks relies digital voting system. The technology guarantees that every vote is permanently recorded by utilizing the Ethereum blockchain additionally Solidity intelligent contracts prohibiting manipulation or unapproved changes. Aadhaar-based voter authentication strengthens eligibility verification, reducing impersonation and duplicate voting, However, the decentralized storage of election papers offered within the Interplanetary the file system. (IPFS) increases resilience towards data loss or breaches. The frontend was created using Semantic UI React and Next.js, offers an intuitive and accessible interface to encourage voter participation. Smart contracts automate vote recording and real-time tallying, minimizing human error and ensuring accurate election results. Rigorous testing—including unit, integration, and functional tests validates system performance, security, and usability. The proposed system demonstrates a practical, scalable approach to modernizing elections, fostering public trust, and supporting the integrity of democratic processes worldwide.

Keywords: Blockchain-based voting, Smart contracts, Aadhaar authentication, Decentralized storage, Election transparency etc.

1. Introduction

Elections are essential to democratic societies because they give people the chance to exercise a fundamental freedom to select their representatives. However, conventional voting systems, whether manual or electronic, have consistently faced significant challenges. Public trust in the voting process is frequently weakened by problems such vote tampering, manipulation, impersonations, lack of transparency, sluggish vote counting, and the possibility of centralized authority meddling. These shortcomings highlight the urgent need for a secure, transparent, and efficient voting mechanism that can safeguard democratic integrity while maintaining voter confidentiality [1].

Blockchain technology has become a game-changer for a number of businesses in recent years, especially those that need high security, accountability, and decentralization. Blockchain is a randomized digital record that keeps track of transactions over a dispersed computer network, guaranteeing that once data is recorded, it becomes immutable and publicly verifiable. The combination of cryptographic security, decentralized storage, and consensus mechanisms makes blockchain an ideal candidate for addressing the vulnerabilities of traditional voting systems. Every transaction of the blockchain has links to the one before it, creating an unchangeable chain that guards against illegal alteration and guarantees data integrity [2][3].

Applying blockchain to electoral systems provides several critical advantages. Firstly, it enhances security, because there is less chance of fraud because votes posted on the decentralized ledger cannot be changed or removed. Second, it guarantees openness by enabling real-time vote verification for all parties involved, including voters, potential candidates, and election officials. Thirdly, blockchain protects voter privacy, allowing people to cast ballots in secret while guaranteeing that every vote is counted correctly. Additionally, important election procedures like voter registration and eligibility verification can be automated using smart contracts, which are algorithms that execute themselves implemented on the blockchain, vote casting, and real-time tallying, minimizing human intervention and reducing the potential for errors [3][4].

The integration of blockchain with modern web technologies further enhances the accessibility and usability of digital voting platforms. For example, Next.js and The semantic user experience React enable an intuitive, interactive, and comfortable user interface that may promote increased voter turnout. Additionally, decentralized storage solutions such as the InterPlanetary File System (IPFS) provide secure storage for election-related files, ensuring resilience against data breaches, loss, or tampering. Combining blockchain with Voter verification is strengthened by Aadhaar-based voter authentication. This reduces the risk of fraud or substitute voting and ensures that voters who are eligible may cast ballots. [5].

Numerous studies have examined blockchain-enabled electronic voting systems, emphasizing advantages such increased voter trust, auditability, and end-to-end verifiability. However, challenges such as scalability, usability, and integration with existing electoral infrastructure remain areas for further research and development. In order to overcome these difficulties, the suggested solution offers a safe, scalable, and transparent digital voting platform suitable for practical deployment [5][6].

In leveraging blockchain technology for elections represents a paradigm shift in how voting systems can be designed to ensure integrity, transparency, security, and efficiency. By combining blockchain, smart contracts, Aadhaar authentication, and decentralized storage, the proposed system offers a robust solution to modernize electoral processes, foster public trust, and strengthen democratic governance [6].

Fig.1. Blockchain based Voting system [5].

2. Literature Survey

A) Literature Review

Wang, et al. (2024), This study presents a blockchain-based e-voting scheme utilizing advanced cryptography and smart contracts on Ethereum. The system ensures end-to-end verifiability, voter privacy, and tamper-proof vote recording. Each vote is securely linked to the blockchain, preventing unauthorized modifications. While the approach demonstrates practical feasibility and strong privacy measures, scalability remains a challenge when applied to large-scale elections. The authors tested the scheme under controlled conditions and highlighted its ability to maintain transparency, integrity, and trust among stakeholders. Overall, this study identifies potential directions to improve the ability to scale and adoption for wider electoral contexts while offering a fundamental basis for enabling private and secure blockchain e-voting.

E. Daraghmi, et al. (2024), VoteChain introduces a public blockchain-based voting platform using smart contracts and Web3 integration. The system emphasizes auditability, transparency, and immutability, allowing voters and administrators to verify results independently. Smart contracts automate vote casting and tallying, reducing human errors. While the platform demonstrates high security and transparency, its applicability to large-scale government elections is limited due to deployment and operational constraints. The study provides a practical model for public blockchain voting, illustrating how decentralization can enhance trust and accountability in elections. The research highlights potential challenges in integration, scalability, and voter accessibility, serving as a benchmark for future blockchain-based electoral systems.

U. Jafar, et al. (2022), This review examines the scalability, privacy, accessibility usability of more than 100 studies involving blockchain electronic voting systems. The study identifies methods like batching, off-chain solutions, and zero-knowledge proofs (ZKPs) to enhance scalability and confidentiality. While blockchain ensures tamper-proof vote recording, practical implementation faces

challenges such as system usability, integration with existing electoral infrastructure, and resource constraints. The authors provide a comparative analysis of various platforms, consensus algorithms, and cryptographic techniques. This work serves as a comprehensive reference for researchers seeking scalable, secure, and privacy-preserving blockchain voting systems. It highlights gaps in adoption strategies and recommends combining on-chain and off-chain approaches for optimal performance.

D. Granata et. al. (2024), The study focuses on Ethereum-based e-voting platforms, employing threat modeling and structured vulnerability assessment. It maps potential risks across voter authentication, smart contracts, and blockchain nodes, proposing mitigation strategies. The research emphasizes risk analysis, attack surface identification, and prevention mechanisms, improving Ethereum e-voting systems' resilience and security. Although the framework works well for finding vulnerabilities, it is primarily Ethereum-specific and less generalizable to other blockchain platforms. The study establishes a systematic approach for auditing smart contracts, securing voter data, and preventing malicious attacks, supplying developers and legislators with useful advice to guarantee the dependability of blockchain-based election systems.

M. J. H. Faruk, et al. (2024), This project suggests a prototype electronic voting system that combines biometric identification and authorization (facial recognition particularly fingerprint scanning) with Hyperledger Fabric. The system ensures secure voter identification, data integrity, and tamper-proof vote storage on a permissioned blockchain. Pilot testing with 100 users demonstrated feasibility and usability, confirming the potential for increased voter confidence. While the prototype highlights strong authentication and privacy, scalability and large-scale deployment remain untested. The study illustrates how combining blockchain and biometrics can improve election security, prevent impersonation, and maintain voter confidentiality, offering a practical approach for future secure, technology-enhanced electoral systems.

S. Basu, et al.(2024), This project creates a blockchain-based electronic voting system specifically for India by combining Ethereum smart contracts with voter authentication based on Aadhaar. The system ensures voter integrity, auditability, and secure vote recording. By linking unique voter identities to blockchain addresses, the platform minimizes fraud and duplicate voting. While the design is context-specific and promising for enhancing election transparency, real-world implementation and testing are limited. The work highlights the feasibility of applying blockchain for secure, decentralized elections in India, offering guidelines for integrating national identity systems, decentralized storage, and smart contracts to enhance trust and efficiency in electoral processes.

B. Vladucu, et al. (2023), This survey analyzes existing blockchain e-voting protocols, comparing privacy, coercion-resistance, verifiability, and performance. It identifies strengths in transparency and security but notes limitations in real-world deployment, user adoption, and scalability. The poll identifies obstacles to integrating blockchain with existing electoral infrastructures and suggests adopting privacy-preserving methods, standardizing protocols, and using hybrid on-chain/off-chain strategies. By synthesizing recent studies, it provides a comprehensive roadmap for researchers and practitioners seeking to design practical, secure, and transparent blockchain-based voting systems.

Bruno Miguel et. al. (2025), This conceptual work outlines an Ethereum-based e-voting platform emphasizing immutability, transparency, and end-to-end verifiability. Smart contracts manage voter registration, vote casting, and real-time tallying. While providing a strong theoretical model for blockchain voting, practical implementation and scalability remain untested. The study contributes a framework for designing secure and verifiable elections using Ethereum, serving as a reference for future development of decentralized electoral systems.

A. Shaikh, et al. (2025), This study proposes a policy-level framework for national-scale blockchain voting in Oman. It addresses governance, regulatory fit, phased adoption, and strategic planning. While conceptual, the work outlines steps for secure, transparent, and accountable elections, emphasizing public trust and compliance with national policies. Technical depth is limited, but the study contributes a roadmap for blockchain integration in governmental electoral systems, highlighting potential socio-political and regulatory considerations for adoption.

B) Literature Summary

- Recent studies confirm that blockchain-based e-voting systems significantly improve security, transparency, and tamper resistance through immutability and cryptographic protection [1][2].
- Ethereum smart contracts enable automated vote casting, verification, and real-time tallying, reducing human intervention and errors [1][4][8].
- Public blockchain platforms enhance auditability and voter trust but face scalability and deployment challenges in large-scale elections [2][7].
- Systematic reviews highlight performance bottlenecks and recommend hybrid on-chain/off-chain models, batching, and zero-knowledge proofs to improve scalability and privacy [3][7].
- Security-focused research identifies vulnerabilities in authentication and smart contracts, proposing structured threat modeling and mitigation strategies [4].
- Permissioned blockchains integrated with biometric authentication strengthen voter identity verification and fraud prevention [5].
- Context-specific systems integrating national IDs, such as Aadhaar, demonstrate feasibility for reducing impersonation but lack extensive real-world validation [6].
- Policy-oriented studies emphasize governance, regulatory compliance, and phased adoption for national-scale implementation [9].

C) Research Gap

- Most blockchain-based e-voting studies emphasize security and immutability but lack robust integration with national identity systems such as Aadhaar for strong voter authentication.
- Limited research evaluates scalability under real-world conditions involving millions of voters and high transaction volumes.
- Many proposed systems remain at conceptual or prototype stages without large-scale pilot testing or deployment.
- User interface design and accessibility for diverse populations are often overlooked, affecting voter adoption.
- The integration of decentralized storage solutions like IPFS for secure electoral data management is insufficiently explored.

• Smart contract-based real-time tallying mechanisms are rarely compared empirically with traditional vote counting systems.
• Few studies conduct comprehensive performance, cost, and security comparisons between traditional and blockchain voting models.
• Legal, regulatory, and policy compliance aspects receive limited attention in technical implementations.

3. Research Methodology

A) Criteria for selecting this study:
• Relevance to Electoral Security:
The study was chosen because it directly uses blockchain technology to enhance the integrity, security, and transparency of contemporary electoral processes.
• Integration of Emerging Technologies:
To ensure a thorough and cutting-edge approach, research that combines cryptocurrencies with contract technology, Web3, IPFS, followed by fingerprint- or Aadhaar-based identity verification was given preference.
• Focus on Scalability and Decentralization:
Studies addressing scalability challenges, decentralized storage, and distributed ledger mechanisms were prioritized for their potential to handle large-scale, real-world elections.
• Practical Implementation and Feasibility:
Selected papers include systems that have been prototyped or tested (e.g., using Ethereum, Hyperledger Fabric, or simulated elections), demonstrating practical feasibility beyond theoretical concepts.
• Security and Privacy Evaluation:
Literature emphasizing vulnerability assessment, encryption models, and privacy-preserving techniques was included to ensure robust security validation.
• Recent and Peer-Reviewed Sources:
Studies from 2022–2025 were prioritized to capture the most current developments and align the methodology with recent research trends and technological standards.

B) Method of analysis:
• Comparative Review of Literature:
A thorough examination of current blockchain-based voting methods is the first step in the investigation. (2022–2025), comparing their technologies, architectures, and security mechanisms to identify common trends and limitations.
• System Architecture Evaluation:
To evaluate the system's performance, scaling, and implementation viability, each model's architectural framework—which includes smart contracts, authentication modules, and blockchain type (public or private)—is examined.
• Privacy and Security Evaluation:
Research is analyzed for the usage of encryption methods, cryptographic algorithms, and privacy-preserving measures including biometric verification and Zero-Knowledge Proofs (ZKP).
• Functional Performance Analysis:

The systems are compared based on transaction speed, throughput, latency, and resource efficiency using metrics from simulation or pilot test data.

- Comparative Strength and Limitation Mapping:

Each study's strengths (e.g., transparency, auditability) and weaknesses (e.g., scalability, user adoption) are mapped to identify improvement areas.

- Synthesis of Findings:

Insights from the reviewed studies are consolidated to propose an optimized blockchain-based voting framework that balances security, transparency, scalability, and usability for real-world electoral applications.

C) Comparison and Analysis:

Title	**Technology Used**	**Security Features**	**Limitations**	**Key Contribution**
An efficient and versatile e-voting scheme on blockchain	Advanced cryptography, smart contracts	End-to-end verifiability, voter privacy	Scalability issues in large-scale deployment	Practical scheme ensuring verifiability & privacy with feasibility evaluation
Decentralizing Democracy: Secure and Transparent E-Voting via Public Blockchain (VoteChain)	Smart contracts, Web3	Auditability, transparency, immutability	Limited focus on large-scale government adoption	VoteChain model emphasizing verifiability & transparency
Scalable blockchain-based electronic voting systems: A systematic review	Meta-analysis of 100+ studies	Privacy-preserving, batching, off-chain solutions	Usability and practical adoption challenges	Comprehensive survey identifying scalability, ZK methods, off-chain optimization
Vulnerability assessment of Ethereum-based e-voting	Threat modelling, vulnerability assessment	Risk mapping, mitigation strategies	Focused on Ethereum only, less generalizable	First structured vulnerability framework for Ethereum e-voting platforms
Transforming online voting with blockchain & biometric verification	Hyperledger Fabric, biometrics (facial, FP)	Biometric verification, secure authentication	Small pilot (100 users), scaling not tested	Prototype combining blockchain and biometrics
Blockchain-powered e-voting in Indian context	Aadhaar integration, smart contracts	Voter integrity, auditability,	Focus on Indian context only; lacks real testing	Context-specific model linking Aadhaar/biometrics

		identity verification		
E-voting meets blockchain: a survey	Survey of blockchain protocols	Privacy, coercion-resistance, transparency	Broad survey without implementation	Highlights open challenges & standards need
Ethereum Blockchain-Based Decentralized Voting Platform	Ethereum, smart contracts	End-to-end verifiability, immutability	Conceptual; lacks practical implementation	Conceptual Ethereum model aligned with verifiability principles
Blockchain-based voting reforms in Oman	Framework for national adoption	Governance fit, phased adoption	Conceptual/policy-level, no technical depth	Policy framework for blockchain voting in Oman

D) Highlighting trends, advancements, and challenges

Trends:
• Increasing adoption of blockchain for secure and transparent e-voting systems.
• Growing use of Ethereum smart contracts for automated vote casting and tallying.
• Shift toward integrating biometric and national ID-based voter authentication.
• Emphasis on end-to-end verifiability and auditability.
• Rising interest in decentralized storage solutions like IPFS.
• Inclusion of policy and governance frameworks for national-level adoption.

Advancements:
• Development of tamper-proof voting using immutable blockchain ledgers.
• Smart contracts enabling real-time vote counting with minimal human intervention.
• Improved voter authentication through biometrics and Aadhaar integration.
• Adoption of hybrid on-chain/off-chain models for better scalability.
• Enhanced privacy through cryptographic hashing and zero-knowledge proofs.
• Improved system security via threat modeling and vulnerability assessment.

Challenges:
• Development of tamper-proof voting using immutable blockchain ledgers.
• Smart contracts enabling real-time vote counting with minimal human intervention.
• Improved voter authentication through biometrics and Aadhaar integration.
• Adoption of hybrid on-chain/off-chain models for better scalability.
• Enhanced privacy through cryptographic hashing and zero-knowledge proofs.
• Improved system security via threat modeling and vulnerability assessment.

4.Discussion

A) Synthesis of findings from literature

The reviewed literature demonstrates that blockchain technology offers a strong foundation for developing secure, transparent, and tamper-proof electronic voting systems. Most studies confirm that the use of Ethereum smart contracts enables automated vote casting, verification, and real-time tallying, significantly reducing human intervention and errors. Research also highlights the effectiveness of cryptographic techniques and decentralized ledgers in preserving voter privacy and ensuring end-to-end verifiability. However, scalability remains a critical limitation, particularly for national-scale elections with large voter populations. Several studies recommend hybrid on-chain/off-chain architectures, batching techniques, and zero-knowledge proofs to overcome performance constraints. Integrating strong authentication mechanisms such as biometrics or national identity systems improves fraud prevention but lacks extensive real-world validation. Overall, the findings indicate that while blockchain-based e-voting is technically promising, further research is required to address scalability, usability, regulatory compliance, and large-scale deployment challenges.

B) Methodology for future research directions

Proposed System:

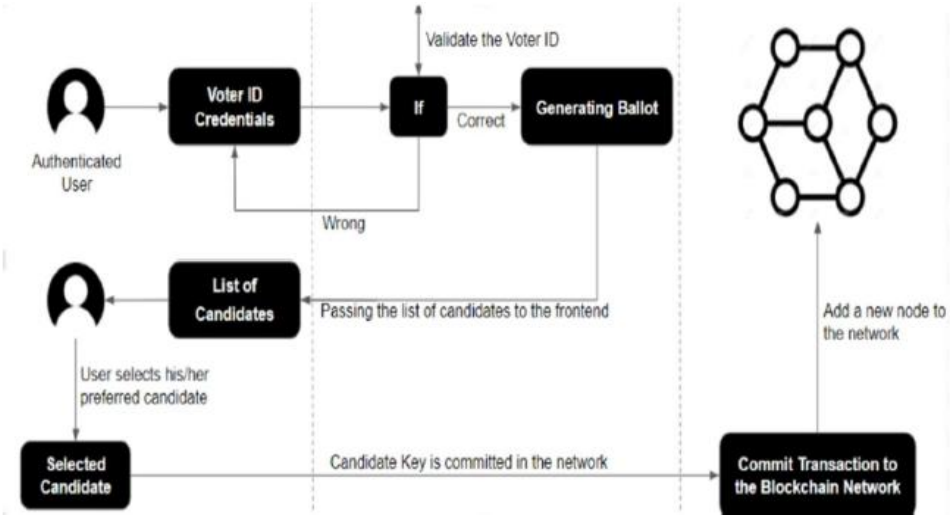

Fig. 2. Proposed system

- Voter Registration – The system uses Aadhaar-based verification for each user's registration. The backend (Node.js + ExpressJS) validates voter identity, and details are securely stored in MongoDB. A unique blockchain wallet address is then linked to the voter.
- Authentication – During login, the system cross-checks Aadhaar details with the stored database to ensure eligibility and prevent duplicate or impersonated voting.
- Ballot Access – After being verified, the voter can view the digital ballot using the Next.js and semantic user React interface.
- Vote Casting – The voter selects a candidate, and the choice is transmitted via Web3.js to the Ethereum blockchain.
- Blockchain Recording – Solidity smart contracts are used to record the vote as an immutable event on the blockchain, ensuring that it cannot be changed or removed.

- Smart Contract Execution – Smart contracts automatically verify voter eligibility, record the vote, and contribute to real-time tallying.
- Decentralized Storage – Election-related files, including ballots and reports, are stored on IPFS for security and scalability.
- Result Declaration – Transparency and trust are ensured by the instantaneous tallying of votes via smart contracts and the public verification of the results in real time.

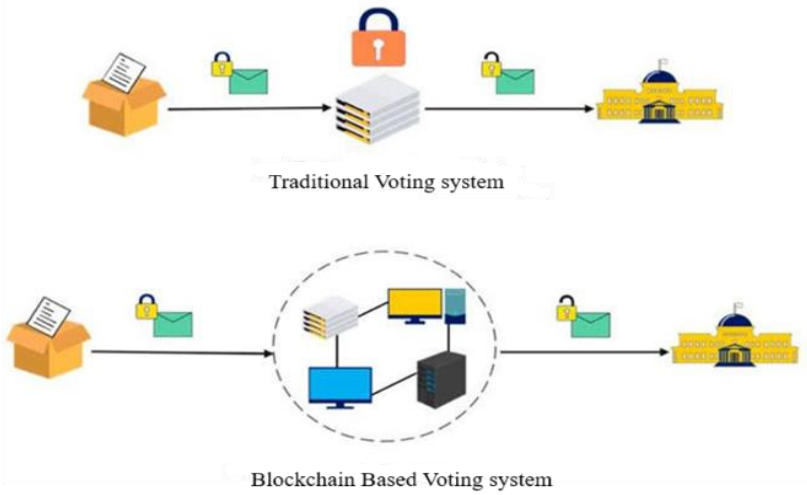

Fig.3. Conventional vs. Suggested Blockchain-Based Voting System

Traditional Voting System:

- After voters cast their voting sheets, they are transmitted to an electoral authority or centralized server.
- Although data is encrypted, the system is susceptible to manipulation, tampering, or unauthorized access because the central authority serves as only one instance of control.
- Election results rely heavily on the integrity of the central server, and any breach can compromise the entire election.
- Transparency is limited as voters and stakeholders cannot independently verify vote counting or tallying.
- The process is prone to delays and human errors during aggregation and reporting of results.

Key Comparison:

- Centralized vs decentralized control.
- Vulnerable vs tamper-proof.
- Limited transparency vs real-time verifiability.
- Manual or error-prone counting vs automated, secure tallying.

Proposed Blockchain-Based Voting System:

- Votes are submitted and recorded on a decentralized blockchain network instead of a single server.
- Multiple nodes (computers/servers) maintain copies of the ledger, ensuring immutability and transparency.

- By handling vote verification, counting and tallying automatically, smart contracts minimize human mistake and manual intervention.
- Voters and election authorities can verify the results in real-time, enhancing trust in the electoral process.
- The system is more resilient to attacks or data manipulation due to its distributed architecture, and voter privacy is maintained.

5.Conclusion

This review examined recent advancements in blockchain-based electronic voting systems, highlighting their potential to overcome critical limitations of traditional voting mechanisms. The literature demonstrates that blockchain technology, particularly when combined with smart contracts, provides strong security, transparency, immutability, and end-to-end verifiability, thereby significantly reducing risks of vote tampering, fraud, and centralized manipulation. Integration of cryptographic techniques, decentralized storage, and advanced authentication mechanisms such as biometrics and national identity systems further strengthens voter trust and data integrity. However, the review also reveals persistent challenges, including scalability constraints, high transaction costs, limited real-world deployment, and usability concerns for diverse voter populations. Legal, regulatory, and policy readiness remain additional barriers to nationwide implementation. Despite these challenges, ongoing research trends toward hybrid on-chain/off-chain architectures, improved consensus mechanisms, and user-centric design indicate promising directions for future development. Overall, blockchain-based e-voting represents a viable and transformative approach to modernizing democratic processes, provided technical, operational, and regulatory issues are systematically addressed through interdisciplinary research and pilot-scale deployments.

References

1. Y. Wang, et al., “An efficient and versatile e-voting scheme on blockchain,” Cybersecurity (SpringerOpen), 2024.
2. E. Daraghmi, et al., “Decentralizing Democracy: Secure and Transparent E-Voting via Public Blockchain (VoteChain),” Future Internet (MDPI), 2024.
3. U. Jafar, et al., “A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems,” Sensors (MDPI), 2022.
4. D. Granata, M. Rak, P. Palmiero, and A. Pastena, “A methodology for vulnerability assessment and threat modelling of an e-voting platform based on Ethereum blockchain,” IEEE Access, 2024.
5. M. J. H. Faruk, et al., “Transforming online voting: a novel system utilizing blockchain and biometric verification,” Cluster Computing (Springer), 2024.
6. S. Basu, et al., “Blockchain-powered e-voting system for secure and transparent elections: a novel approach,” Indian Journal of Science & Technology, 2024.
7. B. Vladucu, et al., “E-voting meets blockchain: a survey,” IEEE Access, 2023.
8. Bruno Miguel Batista Pereira, José Manuel Torres, Pedro Miguel Sobral , Rui Silva Moreira,
9. Christophe Pinto de Almeida Soares and Ivo Pereira, “Blockchain-Based Electronic Voting: A Secure and Transparent Solution” in MDPI, 2023.

10. A. Shaikh, et al., "A model for blockchain-based voting reforms in Oman," F1000Research, 2025.
11. C. C. Albrecht and P. Bichsel, "A secure and anonymous blockchain-based voting system," International Journal of Information Security, vol. 20, no. 5, pp. 897–914, 2021, doi: 10.1007/s10207-020-00538-x.
12. R. Kumar and R. Ranjan, "E-voting system based on blockchain technology," Journal of King Saud University - Computer and Information Sciences, 2021, doi: 10.1016/j.jksuci.2021.06.001.
13. C. Catalini and J. S. Gans, "Some Simple Economics of the Blockchain," National Bureau of Economic Research, 2016. [Online]. Available: NBER.
14. L. Zhang and Q. Wen, "Blockchain technology in e-voting: A survey," IEEE Access, vol. 6, pp. 15130–15143, 2018, doi: 10.1109/ACCESS.2018.2804082.
15. M. A. Khan and M. A. Riaz, "A blockchain-based e-voting system," International Journal of Computer Applications, no. 975, p. 8887, 2020.
16. H. Wang et al., "A blockchain-based voting system for secure electronic voting," Future Generation Computer Systems, vol. 105, pp. 85–93, 2020.
17. M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015.
18. J. Mikulec and R. Haldar, "Blockchain technology and its applications in e-voting," Journal of Cybersecurity and Privacy, vol. 1, no. 1, pp. 1–16, 2019, doi: 10.3390/jcp1010001.
19. J. Katz and Y. Lindell, Introduction to Modern Cryptography: Principles and Protocols. Boca Raton, FL, USA: CRC Press, 2020.
20. J. Zhang and H. Wang, "A survey on blockchain technology for electronic voting," ACM Computing Surveys (CSUR), vol. 53, no. 4, pp. 1–35, 2020, doi: 10.1145/3395055.
21. A. Kumar and A. Singhal, "A framework for blockchain-based electronic voting system," Journal of King Saud University - Computer and Information Sciences, 2019, doi: 10.1016/j.jksuci.2019.06.004.
22. M. Swan, Blockchain: Blueprint for a New Economy, Revised ed. Sebastopol, CA, USA: O'Reilly Media, 2017.
23. C. Gao and P. Liu, "A decentralized voting mechanism based on blockchain technology," Information Sciences, vol. 509, pp. 54–66, 2020, doi: 10.1016/j.ins.2019.08.049.
24. Q. Gong, M. Li, and Y. Guo, "An efficient and secure blockchain-based voting system," IEEE Transactions on Information Forensics and Security, 2021.