STM JOURNALS

Journal of
Network Security

https://journals.stmjournals.com/jons

ISSN: 2395-6739 (Online)
ISSN: 2321-8517 (Print)
Volume 14, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoNS

Review JoNS

Blockchain-Enabled E-Voting Systems: Implementation Challenges and Opportunities

Aniket Roy[1,*], Soumyadip Bhattacharyya[1], Aditi Mandal[1], Sabyasachi Chakraborty[2], Lipi Begam[2]

Abstract

The adoption of blockchain technology in electronic voting systems is increasingly drawing interest because of its ability to enhance transparency, strengthen security, and ensure the reliability of digital voting processes. This study provides a comprehensive study of existing research on e-voting systems that leverage blockchain technology. The study explores various key research concerns, including the advantages, challenges, and impacts of such systems as well as technologies and implementations, and identifies future research directions in this field. The reviewed studies most commonly emphasize security, transparency, and decentralization as the main advantages. By comparison, factors such as privacy, verifiability, efficiency, reliability, and auditability, although addressed, are not treated as central themes. Our analysis also reveals that limited attention is given to aspects like accessibility, compatibility, trustworthiness, and efficiency within existing literature. While these elements are recognized, they are discussed less extensively than the dominant benefits highlighted in proposed blockchain-based e-voting solutions. Nevertheless, the examined works present well-organized frameworks for blockchain-enabled e-voting systems, primarily concentrating on the role of blockchain in strengthening security, transparency, and privacy. Notably, the critical aspect of scalability requires attention in future research endeavors.

Keywords: Blockchain, digital transformation, e-voting systems, scalability, security, transparency

INTRODUCTION

Blockchain technology has emerged as a promising solution for secure and transparent e-voting systems, leveraging decentralization, immutability, and transparency to reduce fraud, enhance voter anonymity, and build trust while lowering costs and time compared to traditional voting [1]. This review evaluates blockchain-based e-voting platforms by examining frameworks, smart contracts, consensus algorithms, and security/privacy measures [2].

Blockchain enables decentralized transaction recording via distributed ledgers, pioneered by Bitcoin and extended by platforms such as Ethereum and Hyperledger Fabric, which support smart contracts for automated agreement execution [3].

Following a review approach, we defined research questions, conducted a literature search, applied inclusion/exclusion criteria, and synthesized findings to provide a descriptive overview of key technologies, benefits, and challenges; identify gaps; and guide future research in blockchain-based e-voting [4].

Structure of the Paper

The following sections delineate the various aspects covered in this paper, offering insights into the evolving landscape of e-voting systems and the role of blockchain technology in shaping the future of democratic processes [5].

***Author for Correspondence**
Aniket Roy
E-mail: royaniket2212@gmail.com

[1]Student, Department of Information Technology, B.P. Poddar Institute of Management and Technology, Kolkata, India
[2]Assistant Professor, Department of Information Technology, B.P. Poddar Institute of Management and Technology, Kolkata, India

Received Date: October 14, 2025
Accepted Date: December 16, 2025
Published Date: February 20, 2026

Citation: Aniket Roy, Soumyadip Bhattacharyya, Aditi Mandal, Sabyasachi Chakraborty, Lipi Begam. Blockchain-Enabled E-Voting Systems: Implementation Challenges and Opportunities. Journal of Network Security. 2026; 14(1): 9–15p.

Section 2. Types of Voting Systems

This section categorizes different voting systems, including e-voting and traditional methods, providing a foundational understanding of the various approaches to conducting elections [6].

Section 3. Voting System Requirements

Here, we delve into the necessities and constraints imposed on e-voting systems during development, distinguishing between functional and non-functional requirements to ensure effective implementation [7].

Section 4. Literature Review

This section reviews the existing literature and research in this field, highlighting gaps and areas for further investigation, with a particular focus on the limitations and advancements in blockchain-based e-voting systems [8].

Section 5. Implementation of Blockchain in E-Voting Systems

Examining the integration of blockchain technology into e-voting systems, this section explores the benefits, challenges, and real-world applications of blockchain-based solutions in electoral processes [9].

Section 6. Research Gap and Objectives

This section outlines the research gap and objectives, emphasizing the need for a comprehensive comparison between blockchain-based e-voting systems and traditional electronic methods [10]. The objectives include analyzing implementation methods, exploring implications, and proposing a roadmap for future research in this evolving field [11].

Section 7. Observation: Benefits of Blockchain-Based E-Voting Systems

This section compares the advantages of blockchain-based e-voting systems with those of traditional methods, aligning them with the requirements specified for e-voting and categorizing them into major requirement groups [12].

Section 8. Results: Technologies and Implementation of Blockchain-Based E-Voting Systems

Here, we summarize the diverse concepts and technologies employed in blockchain-based e-voting systems, including blockchain frameworks, consensus algorithms, smart contracts, security, privacy techniques, and authentication mechanisms [13].

Section 9. Conclusion

In summary, this section underscores the significance of advancing research in secure and transparent e-voting systems, highlighting the contributions made in understanding and implementing blockchain technology in electoral processes [14].

TYPES OF VOTING SYSTEM

Traditional Voting

Conventional voting involves traditional methods in which individuals mark their choices on paper ballots or use mechanical lever machines [15]. These votes were collected and tallied by election authorities. Paper-based voting can be remote, by mail, or on-site at polling stations. Mechanical lever machines, introduced in the 1890s, allow voters to select candidates by activating their levers. Both methods ensure manual vote counting and preparation for the next voter [16].

E-Voting

E-voting uses electronic devices to record, cast, or count votes [17]. This includes several subtypes.

- *Punch-card:* An early system using modified cards where voters punched out cards.

- *Direct recording electronic (DRE):* Record votes directly into computer memory using touch screens or buttons. Some include a voter-verified paper audit trail (VVPAT) [18].
- *Optical filtering frameworks:* Voters fill machine-readable ballots that are scanned using specialized hardware and software.
- *Ballot-marking gadgets (BMDs):* These devices display ballots electronically and produce a human-readable paper ballot without storing the vote electronically [19].
- *Voting:* Also known as online or remote e-voting, this involves transmitting and registering ballots over the internet. Blockchain-based e-voting is a type of i-voting that uses peer-to-peer networks and blockchain technology [20].

VOTING SYSTEM REQUIREMENTS

For e-voting systems to be effective, they must meet specific functional (FR) and non-functional (NFR) requirements, which can be categorized into security and non-security groups.

Non-Security Requirements

Functional Requirements

- *Voter-Focused Voting Design (FR):* The system must be accessible, have a user-friendly interface, and present choices impartially without favoring any candidate [21].
- *Versatility:* This pertains to the system's capability to adjust to various formats, languages, and voting ballots, thereby ensuring compatibility across different platforms and technologies [22]. To offer a versatile and adjustable electronic voting experience, this statement underscores the ability to accommodate modifications, meet deadlines, and support various types of ballot questions, including open-ended queries [23].

Non-Functional Requirements

- *Equality:* "The principle of equality ensures that all voters have fair, consistent access, and equal rights regardless of voting method."
- *Accessibility:* This emphasizes providing individuals with disabilities with full, non-discriminatory access to vote, including logical and physical access to the voting system.
- *Auditability:* This ensures that all votes are accurately tallied and recorded with reliable election records and a permanent audit trail that preserves voter secrecy.

Security Requirements

Functional Requirements

- *Voter authenticity:* This ensures voter identification based on the voter registration database, allowing only eligible voters to cast their votes.
- *Uniqueness:* Guarantees that each voter can submit a vote only once, and the final result of that voter remains immutable.
- *Eligibility:* Ensures that only legitimate voters can vote and verifies their identities accurately.
- *Secrecy:* ensures that no participant in the voting process can correlate a specific ballot to a particular voter, thereby preserving voter anonymity.

Non-Functional Requirements

- *Data protection:* ensures that each vote is securely recorded and tamper-proof, with measures preventing unauthorized access or manipulation [24].
- *System integrity:* Maintains resistance to security failures by preventing reconfiguration during operation and employing multiple levels of control.
- *Reliability:* ensures robust system functionality without losing votes, even in the face of multiple failures, and prevents the introduction of malicious code or bugs.
- *Testing:* Allows thorough testing of voting systems by experts to ensure that they meet the established criteria and security standards.

LITERATURE REVIEW

The developed blockchain-based digital voting system was designed for technologically advanced regions, but security vulnerabilities allowed for potential vote manipulation [25]. highlighted the benefits and challenges of blockchain e-voting, noting issues of scalability, privacy, and system immaturity. The proposed vote accuracy methods use unique voter codes, adding complexity [26].

Analyzed blockchain e-voting systems, discussing strengths, weaknesses, and limitations, such as transaction handling and voter identification. Reviewed blockchain voting, identified security and privacy concerns, and classified blockchain types. surveyed global blockchain e-voting systems, addressed challenges, suggested improvements, and explained key technical mechanisms [27].

IMPLEMENTATION OF BLOCKCHAIN IN E-VOTING SYSTEMS

Blockchain-based e-voting projects include Votem's Cast Iron, managing 13 million voters with audit trails and no breaches, a mobile app with biometric verification but security issues, and ensuring secure, transparent, and verifiable voting via blockchain; certification involves audits, testing, usability, and compliance assessments [28, 29].

RESEARCH GAP AND OBJECTIVES

Despite ongoing research in this domain, existing studies have often focused on the limitations of blockchain-based e-voting, neglecting a comprehensive comparison with traditional and electronic voting systems regarding their merits and challenges [30].

Consequently, the main objectives of this analysis are as follows:

1. Conducting a thorough comparison between blockchain-based e-voting systems and traditional/electronic voting systems according to Section 2, with a focus on understanding their respective advantages and challenges.
2. To review and analyze the specific implementation methods of blockchain technology in e-voting systems, we examine how they address existing challenges in the field.
3. To explore the potential implications of adopting blockchain-based e-voting systems to address the current challenges faced by traditional e-voting systems.
4. To develop an updated roadmap for future research endeavors, key areas require further investigation in the rapidly evolving domain of blockchain-based e-voting.

OBSERVATION

Benefits of Blockchain-Based E-Voting Systems

Several studies have supported the adoption of blockchain-based e-voting systems because of their significant advantages over traditional electronic voting. These systems offer enhanced security, transparency, efficiency, and trustworthiness, meeting the essential e-voting requirements.

Key Benefits

- *Security:* Blockchain ensures that data is tamper-resistant**,** with high integrity throughout the voting process.
- *Immutability:* Votes cannot be altered once recorded.
- *Durability and stability:* Resistant to data loss and cyberattacks.
- *Privacy:* Protects voter identity and vote confidentiality.
- *Decentralization:* Distributes control across a network, reducing the risk of central manipulation.
- *Efficiency:* Streamlines processes like vote casting and counting.
- *Cost, time, and performance efficiency* lead to lower costs and faster results.
- *Trustworthiness:* A transparent and secure system builds public confidence.
- *Compatibility:* Adapts to various technical and legal frameworks.
- *Affordability:* cost-effectiveness in terms of deployment, maintenance, and resource use.

RESULTS

Technologies and Implementation of Blockchain-Based E-Voting Systems

Blockchain-based e-voting systems use various frameworks, including Ethereum and Hyperledger Fabric, along with consensus algorithms, such as Proof of Work, Proof of Stake, and Byzantine Fault Tolerance. Privacy-enhancing techniques, such as homomorphic encryption and zero-knowledge proofs, combined with biometric and identity verification, ensure voter legitimacy and system integrity. The key components include blockchain platforms, consensus algorithms, smart contracts, security and privacy methods, authentication techniques, cryptography, development, and testing tools. Continuous innovations and new consensus mechanisms are expanding blockchain's capabilities in e-voting, addressing security and privacy challenges, and making the sector dynamic and evolving.

Blockchain Platforms

The realm of blockchain frameworks and technologies encompasses a diverse array of platforms and tools essential for crafting and deploying blockchain-driven systems. Foundational frameworks such as Ethereum and Hyperledger Fabric. Bitcoin and MultiChain provide developers with the necessary infrastructure to build decentralized applications. Among the aforementioned frameworks, Ethereum has emerged as the favored option, commanding a substantial portion of the utilized frameworks.

Consensus Algorithms

In e-voting systems, consensus algorithms enable network participants (nodes) to agree on the validity and order of votes on a blockchain without a central authority. They ensure:

- *Validity:* Only legitimate votes are recorded.
- *Integrity:* Votes cannot be altered.
- *Agreement:* All nodes share the same system state.
- *Decentralization:* Operation without a central authority.

Examples of consensus algorithms used in e-voting systems include:

- Proof of work (PoW), used in systems such as Bitcoin, involves miners solving complex computational puzzles to secure the network and verify transactions.
- Proof of stake (PoS) is a consensus mechanism in which validators are selected based on their stake, which serves as collateral to incentivize honesty and secure the network, while high leverage negatively affects stock returns, offering insights for emerging market researchers and policymakers.
- Byzantine fault tolerance (BFT) is a method that achieves consensus among participants even when malfunctioning or malicious nodes are present. BFT consensus algorithms are specifically designed to handle Byzantine failures, in which nodes behave unexpectedly and inconsistently.
- The proof of authority is a consensus mechanism in which trusted, pre-approved validators secure the network and validate blocks.

Smart Contracts

Smart contracts, first conceived in the 1990s, are programmable codes on blockchain that autonomously execute agreement terms without intermediaries, reducing risk and cost, and improving efficiency. E-voting enhances security, transparency, and automation by encoding voting rules on platforms such as Ethereum or Hyperledger Fabric, enabling eligibility verification, vote casting, tallying, and real-time monitoring. Their immutable nature ensures that recorded votes cannot be altered, thus boosting trust and reliability in the electoral process.

Security and Privacy Techniques

Blockchain-based e-voting systems require careful attention to ensure security and privacy. Its decentralized and transparent structure enhances trust and reliability. Incorporating zero-knowledge proofs (ZKPs) allows for verification without revealing sensitive data. ZKPs ensure:

- *Voter privacy:* Vote validity without revealing identity.
- *Vote tallying:* Correct results without exposing individual votes.
- *Ballot integrity:* Ballots are valid and untampered.
- *Voter eligibility:* Confirm eligibility without personal data.
- *Auditing:* Independent verification without compromising confidentiality.

Thus, the ZKPs maintain privacy, integrity, and accurate e-voting outcomes.

Authentication and Identity Verification Techniques

Robust authentication in blockchain-based e-voting using multifactor, multi-step, and biometric verification enhanced by machine learning ensures eligibility, prevents fraud, and secures the system.

CONCLUSION

Blockchain offers a promising solution to traditional e-voting challenges by enhancing security, transparency, trust, and voter anonymity, and reducing costs and time. This review explores various voting systems, their requirements, and related works, highlighting the role of consensus algorithms, ZKPs, and authentication in ensuring system integrity. Despite security challenges, blockchain's potential for revolutionizing e-voting is significant. This paper identifies research gaps, advocates further study, and emphasizes the need for secure, transparent, and trustworthy e-voting systems.

REFERENCES

1. Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ. 2021;372:n71. doi:10.1136/bmj.n71.
2. Stewart C 3rd. Voting technologies. Annu Rev Polit Sci. 2011;14(1):353–378. doi:10.1146/annurev.polisci.12.053007.145205.
3. Breuer F, Trechsel AH. E-voting in the 2005 local elections in Estonia. Report for the Council of Europe. Florence: European University Institute; 2006.
4. Jones DW. The evaluation of voting technology. In: Gritzalis DA, editor. Secure Electronic Voting. Boston (MA): Springer; 2003. p. 3–16. doi:10.1007/978-1-4615-0239-5_1.
5. Congressional Research Service. The direct recording electronic voting machine (DRE) controversy: FAQs and misperceptions. CRS Report. Washington (DC): Members and Committees of Congress, Congressional Research Service; 2007. Available from: https://www.congress.gov/crs_external_products/RL/PDF/RL33190/RL33190.6.pdf
6. U.S. Election Assistance Commission. (2023). Election Technology. [online] U.S. Election Assistance Commission, Washington, DC. Available from: https://www.eac.gov/election-technology
7. Kshetri N, Voas J. Blockchain-enabled e-voting. IEEE Softw. 2018;35(4):95–99. doi:10.1109/MS.2018.2801546.
8. Hajian Berenjestanaki M, Barzegar HR, El Ioini N, Pahl C. Blockchain-based e-voting systems: A technology review. Electronics (Basel). 2023;13(1):17. doi:10.3390/electronics13010017.
9. Gritzalis DA. Principles and requirements for a secure e-voting system. Comput Secur. 2002;21(6):539–556. doi:10.1016/S0167-4048(02)01014-3.
10. Anane R, Freeland R, Theodoropoulos G. E-voting requirements and implementation. The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007), Tokyo, Japan. 2007. p. 382–392. doi:10.1109/CE-CEEE.2007.42.
11. Rathee G, Iqbal R, Waqar O, Bashir AK. On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities. IEEE Access. 2021;9:34165–34176. doi:10.1109/ACCESS.2021.3061411.
12. Hjálmarsson FP, Hreioarsson GK, Hamdaqa M, Hjálmtýsson G. Blockchain-based e-voting system. 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA. 2018. p. 983–986. doi:10.1109/CLOUD.2018.00151.

13. Chaum D, Essex A, Carback R, Clark J, Popoveniuc S, Sherman A, et al. Scantegrity: End-to-end voter-verifiable optical-scan voting. IEEE Secur Priv. 2008;6(3):40–46. doi:10.1109/MSP.2008.70.
14. Jafar U, Ab Aziz MJ, Shukur Z, Hussain HA. A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems. Sensors (Basel). 2022;22(19):7585. doi:10.3390/s22197585.
15. Huang J, He D, Obaidat MS, Vijayakumar P, Luo M, Choo KKR. The application of blockchain technology in voting systems: A review. ACM Comput Surv. 2021;54(3):1–28. doi:10.1145/3439725.
16. Vladucu MV, Dong Z, Medina J, Rojas-Cessa R. E-voting meets blockchain: A survey. IEEE Access. 2023;11:23293–23308. doi:10.1109/ACCESS.2023.3253682.
17. Çabuk UC, Adiguzel E, Karaarslan E. A survey on feasibility and suitability of blockchain techniques for the e-voting systems. [Preprint]. 2020;arXiv:2002.07175. doi:10.48550/arXiv.2002.07175
18. Taş R, Tanrıöver ÖÖ. A systematic review of challenges and opportunities of blockchain for e-voting. Symmetry (Basel). 2020;12:1328. doi:10.3390/sym12081328.
19. Shahzad B, Crowcroft J. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access. 2019;7:24477–24488. doi:10.1109/ACCESS.2019.2895670.
20. Goyal M, Kumar A. Sustainable e-infrastructure for blockchain-based voting system. In: Solanki A, Kumar A, Nayyar A, editors. Digital Cities Roadmap: IoT-Based Architecture and Sustainable Buildings. Hoboken (NJ): John Wiley & Sons; 2021. p. 221–251. doi:10.1002/9781119792079.ch7.
21. Vionis P, Kotsilieris T. The potential of blockchain technology and smart contracts in the energy sector: A review. Applied Sciences. 2023;14(1):253. doi:10.3390/app14010253.
22. Singh A, Ganesh A, Patil RR, Kumar S, Rani R, Pippal SK. Secure voting website using Ethereum and smart contracts. Applied System Innovation. 2023;6:70. doi:10.3390/asi6040070.
23. Díaz-Santiso J, Fraga-Lamas P. E-voting system using Hyperledger Fabric blockchain and smart contracts. Eng Proc. 2021;7:11. doi:10.3390/engproc2021007011.
24. Singh RK, Chaudhary L, Kumar R, Kumar A, Atul A, Bhardwaj ES. Securing elections with blockchain: A review of blockchain-based e-voting systems. 2024 International Conference on Advances in Computing, Communication and Materials (ICACCM), Dehradun, India. 2024. p. 1–6. doi:10.1109/ICACCM61117.2024.11059072.
25. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. Available from: https://bitcoin.org/bitcoin.pdf
26. King S, Nadal S. PPCoin: Peer-to-peer crypto-currency with proof-of-stake. 2012 Aug 19. Available from: https://decred.org/research/king2012.pdf
27. Gągol A, Leśniak D, Straszak D, Świętek M. Aleph: Efficient atomic broadcast in asynchronous networks with Byzantine nodes. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies (AFT '19); 2019; Zurich, Switzerland. New York: Association for Computing Machinery; 2019. p. 214–228. doi:10.1145/3318041.3355467.
28. Visvalingam K, Chandrasekaran RM. Secured electronic voting protocol using biometric authentication. Advances in Internet of Things. 2011;1(2):38–50. doi:10.4236/ait.2011.12006.
29. Qi H, Iyengar SS, Chakrabarty K. Distributed sensor networks – A review of recent research. Journal of the Franklin Institute. 2001;338(6):655–668. doi:10.1016/S0016-0032(01)00026-6.
30. Saini N, Verma H, Sharma P. An analytical study of e-voting system. International Journal of Recent Research Aspects. 2017;4(3):75–85.