International Journal of Basic and Applied Sciences, 14 (6) (2025) 398-401

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/0g3a5r31
Research paper

A Feature Centric Survey of Blockchain-Based E-Voting Systems with Secure QR Authentication and Post-Quantum Cryptographic Enhancement

T. Prabakar *, S. Kanchana

Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Tamil Nadu 603203, India
**Corresponding author E-mail: kanchans@srmist.edu.in*

Received: September 2, 2025, Accepted: October 12, 2025, Published: October 19, 2025

Abstract

The integrity, coupled with the transparency of electoral systems, is vital for the existence of a democratic society if that society is to function well. Often, conventional electronic voting mechanisms are criticized for their security vulnerabilities, with a lack of transparency, together with limited public trust. Blockchain technology has come about to be a possible enabler for trustless and immutable systems. However, such a standard, privacy-preserving, verifiable voting model remains elusive. This work seeks to fill this void with the use of a blockchain e-voting system that uses QR codes to validate voters, cryptographically ensures integrity with the EFFT-SWIFFT hash, and also handles ballots through smart contracts. A feature matrix together with a visual chart was used in a systematic literature review of 28 peer-reviewed papers to analyze and compare authentication methods, transparency techniques, consensus mechanisms, and scalability solutions. Though the analysis reveals that entities greatly underutilize advanced cryptographic primitives such as zero-knowledge proofs and post-quantum hashing, these primitives potentially improve privacy and also verifiability. Present in the proposed model is a multi-layered architecture. Also, the model can offer a secure as well as transparent solution for addressing these gaps. Blockchain-based e-voting can increase trust, reduce fraud, and broaden democratic participation, but it requires real-world validation through pilot projects and usability testing.

Keywords: *Blockchain; Electronic Voting; Smart Contracts; Cryptography; E-Voting Security; Decentralized Systems.*

1. Introduction

Free and equitable elections are a foundation for democratic governance. E-voting systems that are secure and transparent, and that are also tamper-proof, are in higher level of demand as electoral processes become more digitized. Traditional electronic voting systems, while efficient in counting and logistics, are frequently criticized for security loopholes, centralization risks, and the lack of auditability. These challenges erode public confidence and heighten apprehensions regarding electoral integrity, particularly in critical national elections.
Recent advancements in distributed ledger technology (DLT), particularly blockchain, offer, howevertransparency. Blockchain's inherent characteristics, like immutability, transparency, and decentralized consensus, have attracted significant interest among researchers aiming to reimagine electronic voting. Nevertheless, a comprehensive and unified approach that integrates identity verification, vote integrity, and data confidentiality remains largely undeveloped.
This study identifies critical gaps in the current body of literature, particularly the limited use of advanced cryptographic tools (e.g., homomorphic encryption, zero-knowledge proofs, post-quantum hash functions) and the lack of standardized models suitable for real-world deployment. To address this, we propose an enhanced e-voting model that combines QR code-based voter authentication, cryptographically secure EFFT-SWIFFT hashing, and Ethereum-based smart contracts to deliver a verifiable and privacy-preserving voting mechanism.
The methodology involves a detailed literature survey of 28 peer-reviewed papers, filtered through inclusion/exclusion criteria focused on peer-reviewed blockchain-based e-voting implementations from 2018 to 2024. A comparative analysis of technical features was performed to derive trends, research gaps, and emerging practices. These findings intend to inform system design. Future research should also be guided toward more strong, secure, as well as scalable e-voting systems.

2. Related Works

Adiputra et al. [1] suggested a structure for electronic voting using blockchain. Transparency should improve using this system plus vote tampering should be reduced. After votes are submitted, the system ensures they cannot be changed. The system uses decentralized blockchain storage to achieve this guarantee.

Hjálmarsson et al. [2] have developed a blockchain-based e-voting system that is tamper-resistant and transparent. The work stresses smart contracts' use so they ease secure vote tallying as well as verification, maintaining voter anonymity plus decentralization.
Hardwick et al. [3] introduced a privacy-focused blockchain e-voting protocol allowing vote re-casting inside the voting window. Their solution decentralizes, protects voter privacy, and offers mechanisms for transparency and verifiability.
Lee et al. [4] presented an e-voting system; blockchain use prevents ballot tampering plus improves transparency. The paper models an implementation that is suited to small to medium-scale elections and applies the model at a national level. They provide an early prototype but only test small-scale settings. No metrics are reported for large electorates.
Al-Rawy and Elci [5] designed a blockchain-based digital voting system. The design had stressed both transparency and also vote immutability. Their architecture securely frames voter identity when it validates and decentralizes the ledger mechanisms.
Pawlak et al. [6] integrated smart agents into a blockchain-based e-voting system. These agents also assist in decision-making and can improve the automation of voting tasks. The system then has efficiency coupled with security because of these agents.
Yu et al. [7] have proposed such a platform-independent blockchain voting system in which voter privacy and cryptographic verifiability were central to the system. The system employs tools that are advanced cryptographic. They provide for end-to-end security and integrity of vote records.
Sohel Ahmed et.al [8] in their paper introduce an electronic voting system using a hybrid blockchain integrating DeepFace for face recognition, sharding for increased scalability, and post-quantum cryptography techniques improving security. To prevent fraudulent activities as well as to ensure voter privacy, the system employs zero-knowledge proofs with a novel multiparty computation protocol. The system can handle elections on a large scale in a secure way. Analysis indicates its efficient performance potential.
VoteChain, which was designed by Pandey et al. [9], is in fact a blockchain-based electronic voting system that allows for improved election transparency and security. The system diminishes vulnerabilities in regular centralized databases. DoS attacks can affect the use of blockchain technology. The authors implemented and then tested out the system within a real-world polling scenario, and this demonstrated its practical applicability for large-scale elections.
Because of its use of Ethereum smart contracts, Shrestha et al. [10] developed a blockchain-interfaced secure e-voting system. When the system stores votes on the blockchain, it secures them immutably. It features encrypted voter identification with separate portals for voters and election commissions because it seeks to streamline the election process and reduce associated hassles.
Lopes et al. [11] proposed a blockchain-based e-voting system based on blockchain technology's immutable and decentralized nature. Smart contracts are used by the system to ease voting processes that are secure and transparent. This eliminates any need for third-party intermediaries, and it improves efficiency within both public and private sector elections.
Bulut et al. [12] designed a system for electronic voting that is blockchain-based for use in elections in Turkey. The system investigates problems in customary elections such as security vulnerabilities, lack of transparency, and prolonged vote-counting times. Data integrity is guaranteed, voter privacy is safeguarded, with result processing is accelerated by the proposed blockchain solution.
Zhang et al. [13] introduced Ques-Chain, an Ethereum-based e-voting system balancing authentication and confidentiality. The protocol prevents fraudulent activities by ensuring voter anonymity. Authors discuss system adaptability to applications other than voting, too. They do highlight the versatility of the system.
Fatrah et al. [14] have presented a proof-of-concept voting system based on blockchain. Voter privacy, reliability, and security were stressed by the system. To protect voter identities and to ensure voting process integrity, the system incorporates smart contracts and zero-knowledge proofs. Election expenses can be diminished as electoral processes can have a strengthening of trust by way of this system, the authors contend.
Khan et al. [15] suggested a secure online voting system using blockchain, as they sought to improve e-voting system resilience. End-to-end verifiability is achieved since the system leverages blockchain's transparency with cryptographic foundations. The system makes use of the Multichain platform. It works well to make elections secure and clear.
Kumar et al. [16] developed a secure electronic voting system using blockchain technology, where voter details and votes are stored in separate blockchains. This dual-blockchain methodology improves transparency and enables voters to independently audit the ballot box while preserving confidentiality. The system facilitates online voting, making the process more accessible and secure.
Hardwick et al. [17] developed a decentralized blockchain protocol for secure electronic voting, ensuring ballot confidentiality, vote re-casting, and comprehensive verifiability. The approach includes a mix of voter anonymity and blockchain integrity using cryptographic credentials.
Zheng et al. [18] conducted a comprehensive survey of blockchain technologies, including their use in secure e-voting. The paper discusses consensus mechanisms, smart contracts, and decentralized applications, highlighting key research challenges in voting applications.
Chaum et al. [19] introduced Scantegrity, a voting system that adds end-to-end verifiability to traditional optical scan voting. It utilizes cryptographic confirmation codes, allowing voters to verify that their votes were correctly counted.
Hanifatunnisa and Rahardjo [20] developed a blockchain-based e-voting system that integrates SHA-256 and smart contracts for end-to-end security. The prototype demonstrates practical security in vote casting, storing, and verification.
Noizat [21] discussed the potential of blockchain voting systems as an extension of Bitcoin's decentralized architecture. The paper introduces the conceptual framework for blockchain-backed vote recording and auditability, which lays foundational insights into future decentralized voting models.
Kshetri and Voas [22] provided an analytical review of blockchain applications in voting systems. The authors emphasize socio-technical barriers, government trust requirements, and the potential of smart contracts to automate electoral processes while ensuring transparency.
Hjalmarsson et al. [23] proposed a decentralized e-voting model that uses the Tendermint consensus engine for fast, Byzantine-fault-tolerant vote aggregation. Their system separates vote storage from vote tallying to improve both privacy and system performance.
Springall et al. [24] performed a security analysis of the Estonian Internet voting system, uncovering vulnerabilities in vote privacy, server authentication, and malware susceptibility. The study emphasized the importance of operational security and proper code auditing in real-world deployments, showing that cryptography alone cannot eliminate operational risks.
Culnane et al. [25] examined the iVote system used in New South Wales, Australia, identifying flaws in SSL certificate validation and vote anonymization. Their analysis highlights how cryptographic weaknesses can compromise election outcomes even in seemingly secure systems.
Ayed [26] presented a smart contract framework for e-voting systems that can be embedded into Ethereum to ensure automation and transparency. The architecture supports real-time auditing and has been tested for latency and correctness in election scenarios.
Benaloh [27] contributed a pioneering scheme using homomorphic encryption for secure vote aggregation. This foundational work established a framework for many modern encrypted tallying systems in e-voting.

Sandler et al. [28] proposed a coercion-resistant voting protocol based on fake credentials and trapdoor commitments. It allows voters to deny their votes under coercion while enabling cryptographic proof during tallying.

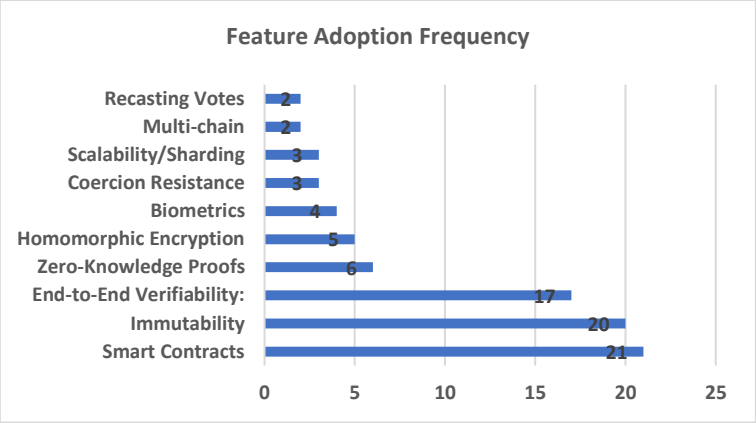

Fig. 1: Feature frequency in Blockchain-based Evoting literature.

Figure 1 illustrates the frequency distribution of ten critical features identified in 28 peer-reviewed papers on blockchain-based electronic voting systems. These features were selected based on their relevance to security, verifiability, usability, and post-quantum resilience. The ten important features are voter authentication, voter anonymity, verifiability, consensus mechanism, smart contracts and automation, scalability solutions, cryptographic primitives, transparency and auditability, coercion resistance, and usability or accessibility. Voter authentication is the process of checking each person's identity using things like biometrics or QR codes. Voter anonymity means that we can't connect a voter's choice to them, and verifiability means that participants and auditors can check that votes were recorded and counted correctly. The system's trust and performance depend on the consensus mechanism it uses, like Proof of Work, Proof of Stake, or Byzantine Fault Tolerance. Automated systems and smart contracts make it possible to program logic for handling and counting ballots. Sharding, layer-2 protocols, and off-chain aggregation methods are all examples of scalability solutions that can handle large electorates. Cryptographic primitives like homomorphic encryption, zero-knowledge proofs, and post-quantum hashing (EFFT-SWIFFT) make security guarantees stronger. Transparency and auditability stress the importance of public ledgers or logs that can be checked, while coercion resistance deals with problems like vote-buying or scaring voters. Finally, usability and accessibility make sure that systems are useful and open to everyone.

Scalability remains a significant challenge for blockchain-based e-voting. Public platforms like Ethereum face high transaction (gas) costs and latency, limiting throughput. Cryptographic components EFFT-SWIFFT also introduce computational overhead depending on the input size. The existing solutions include sharding, layer-2 protocols, and off-chain aggregation with on-chain commitments.

Table 1: Comparison of Scalability Approaches in Blockchain-Based E-Voting Systems

Approach	Mechanism	Pros	Cons
On-chain ballots	Each vote is directly recorded on-chain	Simple audit, strong tamper-evidence	High gas cost, low throughput
Off-chain aggregation + on-chain commitment	Batch votes off-chain, post hash on-chain	Low cost, high throughput	Requires aggregator trust or ZK aggregation
Sharding	Split the electorate across shards	Parallel processing	Cross-shard coordination complexity
Layer-2 (rollups/state channels)	Votes settled off-chain, final state on-chain	Cheap, scalable	More complex, delayed finality
Alternative consensus (Tendermint/BFT)	Use BFT engines in permissioned settings	Low latency, scalable	Requires trusted validators

3. Regulatory and Ethical Considerations

Blockchain-based e-voting systems must follow election regulations that protect the privacy of ballots, make them easy to verify, make sure everyone can vote, and ensure accountability while addressing the challenges of decentralization and data governance. Regulatory frameworks vary across jurisdictions, and permissionless infrastructures may raise other issues like where data is stored, who has authority over it, and responsibility for validator operations. Ethical and social dimensions are equally critical, particularly issues of voter coercion, vote-buying, digital exclusion, and the privacy risks associated with metadata exposure. Implementing coercion resistance mechanisms like deniable credentials, ensuring inclusive design for users with varying digital literacy, and providing accessibility through multiple devices and assistive technologies can enhance fairness and trust. Eventually, transparency must be balanced with privacy; overly detailed audit data can endanger voter anonymity, while insufficient transparency may undermine public confidence in the electoral process.

4. Preliminary Validation

A quick feasibility analysis could strengthen the model's practical relevance. We recommend simulating voting with different numbers of voters (1K, 10K, 100K voters), and then evaluating the cost of gas per batched commitment, the latency of vote submission, and CPU time for EFFT-SWIFFT hashing. Even basic prototype results (e.g., gas ≈ X per 100 votes, latency ≈ Y ms) would show trade-offs and scalability. Future work will augment these tests with full-scale simulations and user trials.

5. Conclusion

Blockchain technology offers a revolutionary potential for enhancing and modernizing electronic voting systems. This survey analyzed over two dozen key contributions, revealing that while the field has made significant strides in design diversity, cryptographic robustness, and privacy-preserving techniques, challenges such as regulatory compliance, voter anonymity, scalability, and coercion resistance remain inadequately addressed. Future work must focus on large-scale usability testing, legal integration, and real-world pilot studies that balance theoretical advances with practical requirements. Collaborative efforts between technologists, policymakers, and civic bodies will be essential for transitioning from proof-of-concept to real-world electoral infrastructure.

References

[1] Adiputra, C. K., Hjort, R., & Sato, H., "A Proposal of Blockchain-Based Electronic Voting System," Proceedings of the 2018 WorldS4 Conference, pp. 22–27, 2018. https://doi.org/10.1109/WorldS4.2018.8611593.

[2] Hjálmarsson, F. P., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G., "Blockchain-Based E-Voting System," 2018 IEEE International Conference on Cloud Computing (CLOUD), pp. 983–986, 2018. https://doi.org/10.1109/CLOUD.2018.00151.

[3] Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K., "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," arXiv preprint, arXiv:1805.10258, 2018. Available at: https://arxiv.org/abs/1805.10258.

[4] Lee, K., James, J. I., Ejeta, T. G., & Kim, H. J., "Electronic Voting Service Using Block-Chain," Journal of Digital Forensics, Security and Law, vol. 11, no. 2, Article 8, 2016. https://doi.org/10.15394/jdfsl.2016.1383.

[5] Al-Rawy, M., & Elci, A., "A Design for Blockchain-Based Digital Voting System," Advances in Intelligent Systems and Computing, vol. 850, Springer, pp. 565–574, 2019.

[6] Pawlak, M., Poniszewska-Marańda, A., & Guziur, J., "Intelligent Agents in a Blockchain-Based Electronic Voting System," Lecture Notes in Computer Science, vol. 11314, Springer, pp. 639–648, 2018. https://doi.org/10.1007/978-3-030-03493-1_61.

[7] Yu, B., Liu, J., Sakzad, A., Nepal, S., Rimba, P., Steinfeld, R., & Au, M. H., "Platform-independent Secure Blockchain-Based Voting System," Cryptology ePrint Archive, Report 2018/657. Available at: https://eprint.iacr.org/2018/657. https://doi.org/10.1007/978-3-319-99136-8_20.

[8] Sohel Ahmed Joni, Rabiul Rahat, Nishat Tasnin, Partho Ghose, Md. Ashraf Uddin, John Ayoade, "Hybrid-Blockchain-Based Electronic Voting Machine System Embedded with Deepface, Sharding, and Post-Quantum Techniques", Blockchains, Vol 2(4), p.366-423, 2024. https://doi.org/10.3390/blockchains2040017.

[9] Pandey, A., Bhasi, M., & Chandrasekaran, K. (2019). VoteChain: A Blockchain-Based E-Voting System. 2019 Global Conference for Advancement in Technology (GCAT), pp. 1–6. https://doi.org/10.1109/GCAT47503.2019.8978295.

[10] Shrestha, R., Sah, R., Shrestha, S., Sarawagi, S., & Adhikari, N. B. (2020). Blockchain Interfaced Secure E-Voting System. Journal of the Institute of Engineering, 15(1), 195–199. https://doi.org/10.3126/jie.v15i1.27730.

[11] Lopes, J., Pereira, J. L., & Varajão, J. (2019). Blockchain Based E-voting System: A Proposal. Proceedings of the 2019 Americas Conference on Information Systems (AMCIS 2019). Available at: https://aisel.aisnet.org/amcis2019/global_dev/global_dev/14/.

[12] Bulut, R., Kantarcı, A., Keskin, S., & Bahtiyar, Ş. (2019). Blockchain-Based Electronic Voting System for Elections in Turkey. arXiv preprint arXiv:1911.09903. Available at: https://arxiv.org/abs/1911.09903.

[13] Zhang, Q., Xu, B., Jing, H., & Zheng, Z. (2019). Ques-Chain: An Ethereum Based E-Voting System. arXiv preprint arXiv:1905.05041. Available at: https://arxiv.org/abs/1905.05041.

[14] Fatrah, A., El Kafhali, S., Haqiq, A., & Salah, K. (2019). Proof of Concept Blockchain-based Voting System. Proceedings of the 4th International Conference on Big Data and Internet of Things (BDIoT'19), pp. 1–5. https://doi.org/10.1145/3372938.3372969.

[15] Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure Digital Voting System Based on Blockchain Technology. International Journal of Electronic Government Research (IJEGR), 14(1), 53–62. https://doi.org/10.4018/IJEGR.2018010103.

[16] Kumar, D. D., Chandini, D. V., & Reddy, D. (2020). Secure Electronic Voting System using Blockchain Technology. International Journal of Smart Home, 14(2), 27–34. https://doi.org/10.21742/IJSH.2020.14.2.04.

[17] Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K., "E-voting with Blockchain: An E-voting Protocol with Decentralisation and Voter Privacy," arXiv preprint arXiv:1805.10258, 2018. Available: https://arxiv.org/abs/1805.10258.

[18] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H., "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data, pp. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85.

[19] Chaum, D., Ryan, P. Y. A., & Schneider, S., "A Practical Voter-Verifiable Election Scheme," Lecture Notes in Computer Science, vol. 3679, Springer, pp. 118–139, 2005. https://doi.org/10.1007/11555827_8.

[20] Hanifatunnisa, R., & Rahardjo, B., "Blockchain-Based E-voting Recording System Design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1–6. https://doi.org/10.1109/TSSA.2017.8272896.

[21] Noizat, T., "Blockchain Electronic Vote," Bitcoin and Cryptocurrency Technologies, Princeton University Press, pp. 1–7, 2015. https://doi.org/10.1016/B978-0-12-802117-0.00022-9.

[22] Kshetri, N., & Voas, J., "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, no. 4, pp. 95–99, 2018. https://doi.org/10.1109/MS.2018.2801546.

[23] Hjálmarsson, F. P., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G., "Blockchain-Based E-voting System," Proceedings of the 2018 IEEE Cloud Computing Conference, pp. 983–986. https://doi.org/10.1109/CLOUD.2018.00151.

[24] Springall, D., Finkenauer, T., Hursti, H., MacAlpine, M., Zach, J., Halderman, J. A., et al., "Security Analysis of the Estonian Internet Voting System," Proceedings of the 2014 ACM Conference on Computer and Communications Security (CCS), pp. 703–715. https://doi.org/10.1145/2660267.2660315.

[25] Culnane, C., Teague, V., & Halderman, J. A., "Security Failures in the iVote System," arXiv preprint arXiv:1504.05646, 2015. Available: https://arxiv.org/abs/1504.05646.

[26] Ayed, A. B., "A Conceptual Secure Blockchain-Based Electronic Voting System," International Journal of Network Security & Its Applications (IJNSA), vol. 9, no. 3, pp. 1–9, 2017. https://doi.org/10.5121/ijnsa.2017.9301.

[27] Benaloh, J., "Verifiable Secret-Ballot Elections," PhD Dissertation, Yale University, 1987. Available: https://www.microsoft.com/en-us/research/publication/verifiable-secret-ballot-elections/.

[28] Sandler, D., Derr, K., & Wallach, D. S., "VoteBox: A Tamper-Evident, Verifiable Electronic Voting System," USENIX Security Symposium, 2008. Available: https://www.usenix.org/legacy/event/sec08/tech/full_papers/sandler/sandler.pdf.