

Review Article

Secure E-Voting Using Blockchain and IoT Integration

Kachhela Dia¹, Yashvi Jivrajani², Aghera Soniya³, Mirani Hemangee⁴

^{1,2,3}Student, V V P Engineering college, India

⁴Student, Shree Swami atmanand saraswati institute of technology Surat, India

DOI: <https://doi.org/10.24321/3051.4282.202503>

I N F O

Corresponding Author:

Kachhela Dia, V V P Engineering college, India

E-mail Id:

diakachhela@gmail.com

Orcid Id:

<https://orcid.org/0009-0009-2775-448X>

How to cite this article:

Dia K, Jivrajani Y, Soniya A, Hemangee M. Secure E-Voting Using Blockchain and IoT Integration. *J Adv Res Oper Syst Dev Evol* 2025; 1(2): 9-11.

Date of Submission: 2025-08-16

Date of Acceptance: 2025-09-06

A B S T R A C T

Electronic voting has long promised speed and convenience, yet concerns over privacy, security, and voter trust remain major obstacles. This survey explores how blockchain technology can transform e-voting into a transparent, tamper-proof, and verifiable system. By leveraging the blockchain's immutability, decentralisation, and cryptographic safeguards, votes can be secured against fraud while preserving voter anonymity. The paper reviews existing blockchain-based e-voting models, highlighting their advantages and challenges, including scalability, usability, and legal adoption. Findings suggest that blockchain has the potential to revolutionise democratic elections, but widespread implementation demands deeper research and real-world validation.

Keyword: Blockchain, Electronic Voting, Secure, Democratic Elections

Introduction

Elections are one of the most important pillars of democracy, yet traditional voting systems—both paper-based and electronic—suffer from challenges such as fraud, tampering, lack of transparency, and high operational costs. Existing centralised e-voting solutions often fail to ensure voter privacy and verifiability, creating mistrust among citizens.^{1,2}

Blockchain technology has emerged as a promising solution to these problems. With its features of decentralisation, immutability, transparency, and security, blockchain can provide tamper-proof records of votes, reduce reliance on intermediaries, and allow end-to-end verifiability. Researchers worldwide have proposed various blockchain-based e-voting models, integrating cryptographic algorithms, the Internet of Things (IoT), and smart contracts to enhance privacy, trust, and efficiency.^{3,4}

This review paper aims to analyse and compare multiple blockchain-based e-voting systems, highlighting their

methodologies, strengths, and limitations. By evaluating different approaches such as VoteChain, crypto-voting, IoT-based models, and smart contract-driven systems, as well as systematic reviews and comparative studies, this paper provides a comprehensive understanding of the current state of blockchain-based e-voting research and its potential for real-world adoption.

This review looks at a range of blockchain voting models—like VoteChain, Crypto-voting, and others—and compares how they work, their advantages, and their limitations. The goal is to better understand the current state of blockchain-based voting systems and explore how close we are to using them in real elections. By analysing these systems, this paper also helps highlight what still needs to be improved for blockchain voting to become a practical and reliable option in the real world.

Literature Survey

Recent research has explored the growing potential of blockchain technology in improving services within

smart cities. Its core features—such as transparency, decentralisation, security, and democratic governance—make it an ideal tool for building trust in digital systems. One of the most promising areas of application is electronic voting. Researchers have proposed blockchain-based voting models that can ensure secure, tamper-proof, and verifiable elections. In particular, Ethereum-based smart contracts have been suggested as a way to enable transparent vote handling while protecting voter data. These systems not only improve security but also enhance public confidence in the electoral process, showing how blockchain could play a key role in the digital future of smart cities.⁶

Building on this foundation, several studies have focused specifically on blockchain-based e-voting systems. The current review looks at the advantages these systems offer, the challenges they face, and the technologies they incorporate. It also examines the impact these systems could have and identifies areas where more research is needed. A systematic review approach was used to select and analyse relevant academic sources, ensuring a well-rounded understanding of the field. Special attention is given to how these systems address essential concerns like transparency, voter privacy, system security, and decentralisation.⁷

Does it Provide Anonymity?

Different electronic voting systems use various technologies to ensure secure and reliable voting. For instance, systems that use biometric Aadhaar verification rely on fingerprint scanners linked to Aadhaar cards. These systems offer proper user authentication and voter verification but are only partly decentralised. Similarly, fingerprint-based systems that use IoT technology also support voter verification through hardware devices, though they aren't fully decentralised either.⁷

Some modern platforms, like those using permissioned blockchain technology, are more secure and decentralised. These software-based systems provide both authentication and voter privacy. One example is the Civitas system, which is built using Java and allows for decentralised and anonymous voting.⁸

On the other hand, platforms like "Follow My Vote" are web-based and do not support anonymity or decentralisation, as they run on centralised systems. Estonia's national voting system, which uses eID cards for authentication, is software-driven and supports both voter verification and partial decentralisation.⁹

Postal voting systems such as DVBM and iVote offer some level of authentication and voter verification, although their degree of decentralisation isn't always clear. Norway's iVoting model uses a MiniID for authentication and includes some decentralisation and privacy features.¹⁰

An interesting research-based system is Votebook, created by New York University. It runs on permissioned blockchain and focuses on secure, decentralised, and private digital voting, making it a strong candidate for future election systems.¹¹⁻¹⁴

In summary, while voter authentication and verification are essential to prevent fraud, maintaining voter anonymity is equally important to protect privacy and prevent coercion. Emerging blockchain technologies offer promising solutions to achieve both, but many existing systems still face challenges in fully ensuring voter anonymity.

Conclusion

The reviewed studies collectively demonstrate that blockchain offers a secure, transparent, and trustworthy foundation for modern e-voting systems. Approaches such as VoteChain emphasise tamper-proof records and voter anonymity, while IoT-integrated solutions aim to optimise data exchange. Models like crypto-voting use advanced cryptographic techniques (e.g., Shamir's Secret Sharing) to further strengthen privacy and resistance against brute-force attacks. Comparative and review papers highlight blockchain's potential to reduce fraud, ensure verifiability, and simplify voting processes.

However, despite these advantages, several challenges remain unresolved. Issues such as Scalability, cost of implementation, computational overhead, voter usability, and legal acceptance still limit large-scale deployment. Most proposed systems are either theoretical models or tested in limited experimental environments and therefore require more real-world trials.

In conclusion, blockchain-based e-technologies like IoT, zero-voting, and promising knowledge proofs and artificial direction for the future of digital intelligence to achieve secure democracy, but practical adoption, efficiency, and universal trust will depend on addressing election systems. scalability, privacy, and regulatory hurdles. Future research should focus on hybrid models combining blockchain with emerging technologies.

References

1. Pandey A, Bhasi M, Chandrasekaran K. VoteChain: a blockchain based e-voting system. In 2019 Global Conference for Advancement in Technology (GCAT) 2019 Oct 18 (pp. 1-4). IEEE.
2. Alam A, Rashid SZ, Salam MA, Islam A. Towards blockchain-based e-voting system. In 2018 international conference on innovations in science, engineering and technology (ICISSET) 2018 Oct 27 (pp. 351-354). IEEE.
3. Hjálmarsson FP, Hreiðarsson GK, Hamdaq M, Hjálmtýsson G. Blockchain-based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) 2018 Jul 2 (pp. 983-986). IEEE.

4. Fusco F, Lunesu MI, Pani FE, Pinna A. Crypto-voting, a Blockchain based e-Voting System. In KMIS 2018 Sep (pp. 221-225).
5. Taş R, Tanrıöver ÖÖ. A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry*. 2020 Aug 9;12(8):1328.
6. Hajian Berenjestanaki M, Barzegar HR, El Ioini N, Pahl C. Blockchain-based e-voting systems: a technology review. *Electronics*. 2023 Dec 19;13(1):17.
7. Sahib RH, Al-Shamery ES. A review on distributed blockchain technology for e-voting systems. In *Journal of Physics: Conference Series* 2021 Feb 1 (Vol. 1804, No. 1, p. 012050). IOP Publishing.
8. Salman SA, Al-Janabi S, Sagheer AM. A review on e-voting based on blockchain models. *Iraqi journal of science*. 2022 Mar 30:1362-75.
9. Sohrabi-Haghighat MH, Mansouri S. Where is my vote?. ICT politics in the aftermath of Iran's presidential election. *International Journal of Emerging Technologies and Society*. 2010;8(1):24-41.
10. Garg K, Saraswat P, Bisht S, Aggarwal SK, Kothuri SK, Gupta S. A comparative analysis on e-voting system using blockchain. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) 2019 Apr 18 (pp. 1-4)*. IEEE.
11. Rao U, Nair V. Aadhaar: governing with biometrics. *South Asia: Journal of South Asian Studies*. 2019 May 4;42(3):469-81.
12. Aneja S, Aneja N, Islam MS. IoT device fingerprint using deep learning. In *2018 IEEE international conference on internet of things and intelligence system (IOTAIS) 2018 Nov 1 (pp. 174-179)*. IEEE.
13. Helliar CV, Crawford L, Rocca L, Teodori C, Veneziani M. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*. 2020 Oct 1;54:102136.
14. Springall D, Finkenauer T, Durumeric Z, Kitcat J, Hursti H, MacAlpine M, Halderman JA. Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014 Nov 3 (pp. 703-715)*.