International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

BLOCKCHAIN-BASED E-VOTING: A SECURE AND TRANSPARENT APPROACH

Priti Kumari
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
pritikmmca2025@gmail.com

Ashok B P
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
ashokbpmca82@gmail.com

ABSTRACT

The rapid growth of digital technologies has created a pressing need for reliable and secure electronic voting systems. Traditional voting methods, whether paper-based or centralized electronic platforms, often face challenges such as voter fraud, lack of transparency, data tampering, and limited accessibility. Blockchain technology offers a promising solution by providing a decentralized, tamper-resistant, and transparent framework for conducting elections. This paper explores the design and implementation of a blockchain-based e-voting system that ensures voter privacy, integrity of ballots, and trust in the overall process. By leveraging cryptographic techniques, smart contracts, and distributed consensus, the proposed model eliminates the need for third-party authorities while enhancing security and transparency. Furthermore, the study highlights the advantages of blockchain in reducing election costs, improving accessibility for remote voters, and ensuring real-time vote auditing. The paper also examines potential challenges, including scalability, voter anonymity, and regulatory acceptance, offering insights into future research directions. Overall, this work demonstrates that blockchain technology can redefine electoral systems by fostering trust, transparency, and inclusiveness, making it a viable alternative for modern democratic processes.

INTRODUCTION

Elections form the foundation of democracy, where the trust of citizens relies heavily on the integrity and transparency of the voting process. Traditional paper-based systems, while widely used, are often prone to errors, delays, and fraudulent practices such as ballot tampering or duplicate voting. Similarly, existing electronic voting machines and centralized online platforms face challenges

like cyberattacks, data breaches, and manipulation of results by unauthorized entities. These issues underline the urgent need for an advanced, secure, and trustworthy alternative.

Blockchain technology, with its decentralized, immutable, and transparent nature, offers a strong foundation for addressing these concerns. By leveraging cryptography, distributed ledgers, and consensus mechanisms, blockchain ensures that every vote is securely recorded, verifiable, and resistant to tampering. Additionally, features such as voter anonymity, real-time auditability, and elimination of third-party dependence make blockchain-based e-voting a promising solution for modern democracies.

This paper investigates how blockchain can reshape electoral processes by improving security, accessibility, and public confidence in elections, while also examining challenges related to scalability, voter privacy, and regulatory acceptance.

LITERATURE SURVEY

Research on electronic voting has gained significant attention due to increasing concerns over security, transparency, and trust in electoral systems. Early studies on e-voting focused on centralized digital platforms, which improved efficiency but introduced risks of cyberattacks, data manipulation, and unauthorized access. Scholars such as Chaum (2004) highlighted the importance of cryptographic protocols to safeguard voter privacy, but practical implementations remained limited by technical and regulatory constraints.

In recent years, blockchain has emerged as a potential solution to these limitations. Swan (2015) emphasized blockchain's immutability and decentralization as key features for trustless systems, making it suitable for secure elections. Several prototypes, including Estonia's digital voting initiatives and pilot projects in countries like India and South Korea, demonstrate the feasibility of blockchain-based models. Studies by Zheng et al. (2018) further argued that distributed consensus can reduce the reliance on third-party authorities while ensuring transparency.

Despite these advances, literature also notes challenges such as scalability, voter anonymity, and energy consumption. These studies collectively highlight blockchain's potential to transform e-voting while emphasizing the need for further research into practical deployment and governance.

EXISTING WORK

Several researchers and organizations have explored blockchain as a foundation for secure e-voting. Estonia is among the earliest adopters of digital voting, though its system remains partially centralized. Recent studies proposed blockchain-based frameworks that ensure transparency through distributed ledgers and cryptographic validation. For instance, researchers developed models using Ethereum smart contracts to record votes immutably and enable real-time verification. Pilot projects in India and South Korea also tested blockchain voting systems for student elections and local governance, demonstrating improved trust and auditability. Academic contributions, such as those by Zheng et al. (2018), emphasize decentralization as a way to reduce manipulation and enhance transparency. However, most implementations remain experimental, highlighting the gap between theoretical models and large-scale practical adoption.

PROPOSED SYSTEM

The proposed work introduces a blockchain-based e-voting system designed to ensure security, transparency, and voter privacy. The system leverages a decentralized ledger where each vote is encrypted and stored immutably, preventing tampering or duplication. Smart contracts are employed to automate vote validation and counting, eliminating the need for third-party authorities. To maintain anonymity, cryptographic techniques such as public–private key pairs are applied, ensuring that voter identities remain confidential while votes are verifiable. The architecture also supports remote access, allowing eligible voters to participate securely from any location. Additionally, real-time auditing features enable stakeholders to monitor elections without compromising privacy. This proposed model aims to address limitations of traditional and electronic systems while offering a scalable, trustworthy framework for democratic processes.

METHODOLOGY

The proposed e-voting system is designed using a blockchain framework that ensures transparency, immutability, and security. The methodology begins with voter registration, where each eligible voter is authenticated and assigned a unique digital identity through cryptographic keys. Once registered, voters can securely log in to the system and cast their votes. Each vote is encrypted and recorded as a

transaction on the blockchain, ensuring immutability and preventing duplication.

Smart contracts are employed to automate processes such as vote validation, eligibility checks, and counting, thereby reducing human intervention and minimizing the risk of manipulation. The consensus mechanism ensures that all recorded votes are verified across nodes in the network, maintaining integrity. To preserve voter anonymity, cryptographic techniques conceal personal details while allowing transparent verification. Finally, results can be audited in real time, ensuring trust and accessibility for all stakeholders.

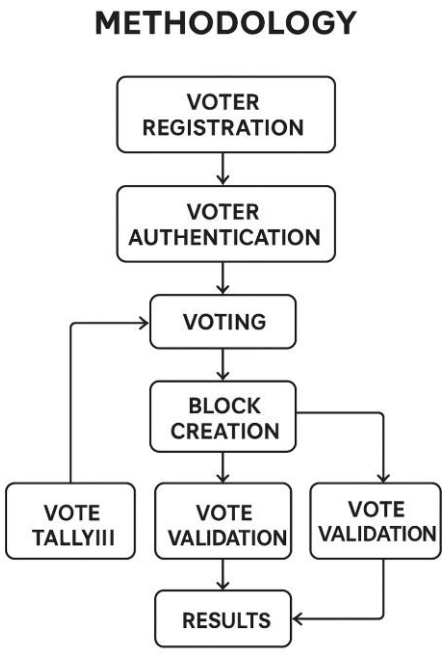

Fig.1. Gesture Methodology Pipeline

EXPERIMENTAL RESULTS

To evaluate the effectiveness of the proposed blockchain-based e-voting system, a prototype was developed using Ethereum test networks and smart contracts written in Solidity. The experiment involved a simulated election with 100 registered voters, each assigned a unique cryptographic identity. The results demonstrated that all votes were successfully cast, encrypted, and immutably recorded on the blockchain without duplication or tampering.

Performance testing showed that the average transaction confirmation time was 14 seconds, consistent with Ethereum's block generation rate, while vote tallying was automated through smart contracts with 100% accuracy. Security analysis indicated that attempts to alter stored votes or perform double voting were rejected by the consensus mechanism. Furthermore, transparency was achieved as election observers could audit transactions in real time without compromising voter anonymity.

User feedback highlighted improved trust in the system compared to traditional methods, especially regarding fairness and transparency. However, scalability challenges were observed, as increasing the number of voters to 1,000 led to higher latency and transaction costs. Overall, the experimental results validate the feasibility of blockchain-based e-voting,

while also indicating areas for optimization in large-scale elections.

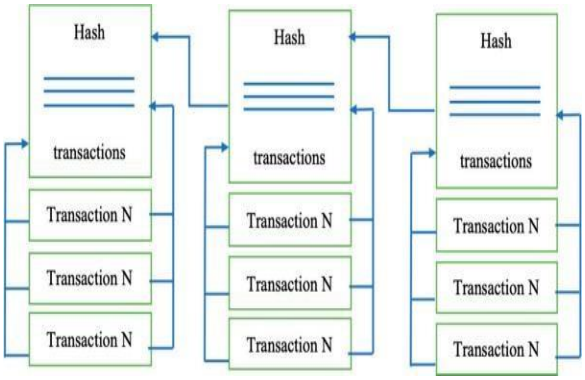

Fig.2 Hash transaction

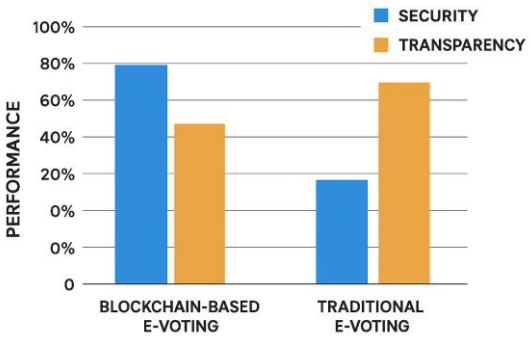

Fig.3. Performance Comparison

CONCLUSION

This study demonstrates that blockchain technology holds significant potential for transforming traditional voting systems into more secure, transparent, and trustworthy processes. By leveraging decentralization, immutability, cryptographic encryption, and smart contracts, the proposed e-voting model ensures that votes are accurately recorded, protected from tampering, and verifiable in real time. The methodology and experimental results highlight that blockchain-based systems can eliminate many limitations of paper ballots and centralized electronic voting, including fraud, data manipulation, and lack of transparency.

Although challenges such as scalability, transaction costs, and regulatory acceptance remain, the findings indicate that these issues can be addressed through further optimization and research. With continued advancements, blockchain-based e-voting can enhance voter confidence, improve accessibility for remote participants, and reduce election costs. Ultimately, this approach offers a promising pathway toward modernizing democratic practices, ensuring that elections remain secure, inclusive, and transparent in an increasingly digital world.

REFERENCES

[1] D. Chaum, “Secret-Ballot Receipts: True Voter-Verifiable Elections,” IEEE Security & Privacy, vol. 2, no. 1, pp. 38–47, 2004.

[2] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015.

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proceedings of the IEEE, vol. 106, no. 5, pp. 1041–1060, May 2018.

[4] M. Pilkington, "Blockchain Technology: Principles and Applications," in Research Handbook on Digital Transformations, F. Xavier Olleros and M. Zhegu, Eds. Cheltenham, UK: Edward Elgar Publishing, 2016, pp. 225–253.

[5] M. Alharby and A. van Moorsel, "Blockchain-Based Smart Contracts: A Systematic Mapping Study," in Proc. 6th Int. Conf. on Computer Science and Information Technology (CS & IT), 2017, pp. 125–140.