Mambilla Journal of Science and the Environment Vol. 9, Issue 3, Page No. 1-6

MAMBILLA JOURNAL OF SCIENCE AND THE ENVIRONMENT

journal homepage: https://oer.tsuniversity.edu.ng/index.php/mjse

BLOCKCHAIN TECHNOLOGY AS A FRAMEWORK FOR SECURE AND TRANSPARENT E-VOTING SYSTEMS

[1*]Ikwuoche, O.L., [2]Garba, E.J.

[1]Department of Computer Science, Taraba State University, Jalingo, Nigeria.
[2] Department of Computer Science, Modibbo Adama University, Yola, Nigeria.

ARTICLE INFO

Article history:
Received 25 September 2025
Received in revised form 15 October 2025
Accepted 20 October 2025

Keywords:
Blockchain, electronic voting, transparency, decentralization, election integrity, cryptography.

ABSTRACT

The credibility of democratic elections hinges on secure, transparent, and verifiable voting systems. Traditional electoral processes, while valued for their physical auditability, suffer from vulnerabilities such as human error, ballot manipulation, and high operational costs. Electronic voting systems emerged to improve efficiency and accessibility but remain susceptible to cyber threats, fraud, and lack of transparency. Blockchain technology has been proposed as a viable solution to these issues, offering decentralization, immutability, and end-to-end verifiability. This paper explores blockchain as a framework for secure and transparent e-voting. Drawing from empirical studies and conceptual models, the paper critically reviews blockchain-enabled voting frameworks, consensus mechanisms, and cryptographic innovations. Results highlight blockchain's potential to enhance voter anonymity, prevent double voting, and ensure election integrity. However, challenges persist in scalability, regulatory compliance, and inclusivity. The study concludes that blockchain-based voting holds promise for strengthening democratic processes but requires technical, legal, and social refinements before large-scale deployment.

1. Introduction

Elections form the bedrock of democratic governance, enabling citizens to select representatives and express political will. However, the trustworthiness of electoral processes is under increasing scrutiny globally, largely due to weaknesses in existing voting systems. Traditional paper-based voting methods are widely trusted because of their tangibility and auditability, yet they are resource-intensive, prone to ballot mismanagement, and inefficient during counting and verification stages (Shneider, 2017; Fischer *et al*., 2016). In developing countries, these systems are further constrained by logistical challenges, inadequate security, and voter intimidation, which undermine democratic legitimacy.

The introduction of Electronic Voting Systems (EVS) promised to alleviate these inefficiencies by digitizing registration, casting, and tallying processes. While such systems enhanced speed and accessibility, particularly through innovations like optical scan ballots and Direct Recording Electronic (DRE) machines, they introduced new risks. Cyberattacks, system malfunction, and the absence of verifiable audit trails have eroded trust in many EVS deployments (Debant & Hirschi, 2023; AlZain *et al*., 2024). The Florida election recount in 2000, for example, highlighted the vulnerabilities of punch card systems, while Brazil's experience with DRE showcased efficiency but suffered criticism for lack of transparency (Herron & Sekhon, 2003; Saldanha & da Silva, 2020).

Blockchain technology, initially designed to power cryptocurrencies, has rapidly evolved into a disruptive tool across finance, healthcare, and governance. Its fundamental properties which include decentralization, immutability, and transparency—are aligned with the requirements of secure voting (Crosby *et al*., 2016; Kushwaha & Singh, 2020). By storing votes as blocks in a distributed ledger, blockchain can mitigate vote tampering, provide verifiable audit trails, and eliminate reliance on centralized electoral authorities. Smart contracts further automate vote tallying, reducing human error and increasing trust (Benaloh *et al*., 2013).

* Corresponding author: +2348066891215
E-mail address: ikwuochel@gmail.com

1.1 Statement of the Problem

Despite advancements in electronic voting, global elections remain vulnerable to manipulation, lack of transparency, and technical inefficiencies. Traditional voting is slow and expensive, while electronic systems face credibility challenges due to cyber risks and inadequate accountability mechanisms. Voter confidence, essential to democracy, is consequently eroded. Blockchain offers a technological remedy, yet its application in elections is nascent and faces significant obstacles such as scalability limitations, energy consumption, legal uncertainty, and challenges in inclusivity (Tas & Tanrıöver, 2020; Jafar *et al*., 2021).

1.2 Objectives of the Study

This paper seeks to:

i. Examine the limitations of traditional and electronic voting systems.
ii. Explore blockchain's potential as a framework for secure and transparent e-voting.
iii. Critically review consensus mechanisms and cryptographic protocols relevant to blockchain voting.
iv. Highlight challenges, research gaps, and opportunities for future implementation.

2. Literature Review

2.1 Traditional Voting Systems

Traditional voting, characterized by the use of paper ballots, has been the backbone of democracy for centuries. Advocates argue that physical ballots offer inherent transparency because they can be independently verified and recounted in case of disputes (Shneider, 2017). However, this tangibility comes with drawbacks such as high operational costs, logistical difficulties in transporting and safeguarding ballots, and vulnerabilities to ballot stuffing or mismanagement (Fischer *et al*., 2016). Moreover, in large-scale elections, the manual nature of counting prolongs results announcement, sometimes fueling post-election tensions. As Debant and Hirschi (2023) argue, the trade-off between transparency and efficiency defines the limitations of traditional systems.

2.2 Electronic Voting Systems (EVS)

Electronic systems emerged as a response to inefficiencies in manual voting. Punch card systems, once considered innovative, failed during the 2000 U.S. election due to ambiguous results from incomplete punches, commonly referred to as "hanging chads" (Herron & Sekhon, 2003). Optical scan voting, adopted widely in the early 2000s, improved efficiency by allowing electronic counting of paper-marked ballots, combining transparency with speed (Ashenfelter, 2018).

Direct Recording Electronic (DRE) systems, implemented in Brazil, showcased the potential of full digitization. The system enabled fast results and minimized fraudulent activities but lacked a paper audit trail, leading to questions of accountability (Saldanha & da Silva, 2020; Brunazo & Amílcar, 2014). Internet voting (i-voting) represents the most advanced form of EVS, pioneered by Estonia in 2005. It facilitated global participation, particularly for diaspora voters, yet heightened risks of voter coercion, cyberattacks, and exclusion of digitally marginalized citizens (Michae *et al*., 2015; Appel, 2023).

Biometric systems, adopted in India and Ghana, reduced impersonation and duplicate registrations (Effah & Debrah, 2018; Mohammad *et al*., 2024). Nonetheless, privacy concerns regarding biometric data storage remain significant (Schroeder, 2016). Table 1 compares traditional, electronic, and blockchain-based systems, highlighting their respective strengths and weaknesses.

Table 1: Comparative Features of Traditional, Electronic, and Blockchain-Based Voting Systems (*adapted from Debant & Hirschi, 2023; Salem et al., 2023b*)

Feature	Traditional Voting	Electronic Voting	Blockchain Voting
Transparency	High (paper trail)	Medium (audit trails vary)	Very high (immutable ledger)
Efficiency	Low	High	High (but scalability issues)
Security	Medium (human error, fraud)	Medium (cyber risks)	High (cryptographic)
Cost	High	Medium to high	High initial, lower ongoing
Inclusivity	Moderate	Moderate	Potentially high (hybrid models)

2.3 Blockchain Voting Systems

Blockchain introduces a decentralized structure that addresses many EVS shortcomings. Votes are stored as immutable blocks across multiple nodes, ensuring tamper resistance and verifiability (Tapscott & Tapscott, 2017). Case studies demonstrate its promise: Kamal *et al*. (2023a) integrated smart contracts on Ethereum to automate tallying

and preserve anonymity; Salem *et al*. (2023b) proposed a Libyan framework combining blockchain with biometric authentication; and Vishal and Amit (2022) applied OTP authentication for enhanced verification.
However, adoption challenges persist. Fajri *et al*. (2020a) found blockchain systems complex for average voters, while Bartolucci *et al*. (2018) highlighted risks of over-reliance on trusted authorities in hybrid designs. Scalability and legal constraints further hinder full adoption, especially in large democracies (Ahmed, 2017; Devi & Bansal, 2023). Figure 1 illustrates a generic blockchain voting architecture, showcasing how authentication, vote casting, and tallying integrate with distributed ledgers.

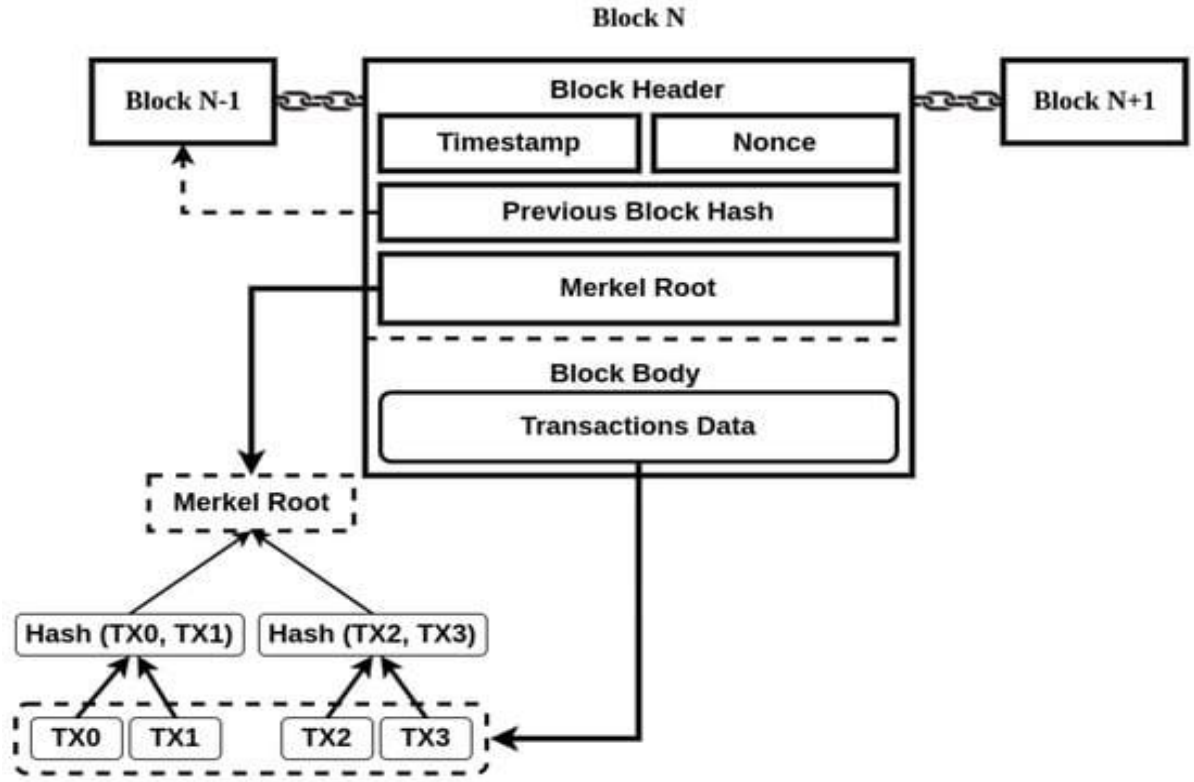

Figure 1: General Architecture of a Blockchain-Based Voting System
(*adapted from Benaloh et al., 2013; Kamal et al., 2023b*)

2.4 Consensus Mechanisms and Cryptographic Protocols

Consensus mechanisms are the backbone of blockchain networks. Proof of Work (PoW), used in Bitcoin, ensures high security but consumes enormous energy (Alhat, 2024). Proof of Stake (PoS) mitigates energy use but risks centralizing control in wealthy participants (Verma *et al*., 2024). Delegated Proof of Stake (DPoS) increases efficiency but reduces decentralization (Diamond, 2023), while Practical Byzantine Fault Tolerance (PBFT) offers high throughput in permissioned systems (Verma *et al*., 2024).
Cryptographic protocols further enhance security. Zero-Knowledge Proofs (ZKPs) enable verification of votes without revealing voter choices, while Homomorphic Encryption allows tallying without decrypting votes (Benaloh *et al*., 2013; Anita *et al*., 2020). Systems like Helios and Scantegrity operationalize these techniques, though complexity remains a barrier to mass adoption (Park, 2019). Figure 2 summarizes key consensus algorithms used in blockchain systems.

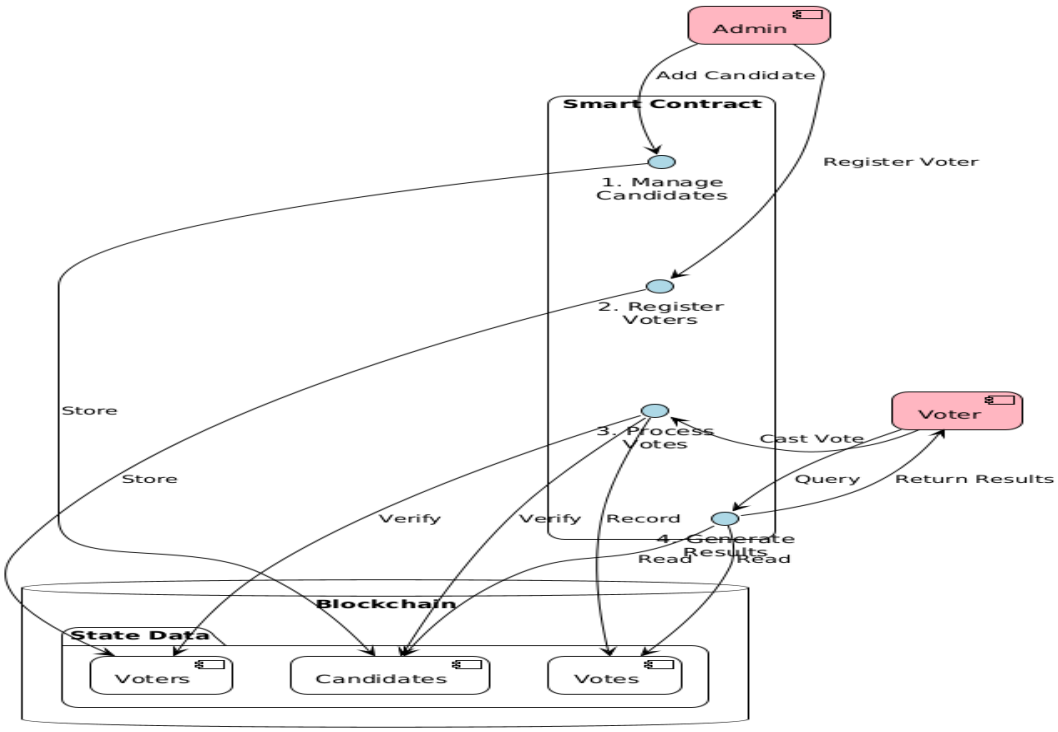

Figure 2: Consensus Mechanisms in Blockchain Networks
(*adapted from Verma et al., 2024; Alhat, 2024*)

3. Methods

This study employed a qualitative exploratory research design, combining literature synthesis with prototype development. The framework was structured in three layers: a **frontend** developed in React for user interaction; a **workflow layer** consisting of Ethereum smart contracts for authentication, vote casting, and tallying; and a **backend** implemented with Python Flask to manage integration with blockchain records.

Security was ensured through asymmetric encryption for vote casting and OTP verification for authentication. Ethereum's Proof of Work (PoW) was used as the consensus mechanism. Testing included simulation of concurrent voting scenarios, evaluation of vote immutability, and analysis of system transparency through blockchain audit logs. Expert feedback was solicited from blockchain specialists and electoral officers to validate the framework's applicability.

4. Results and Discussion

The prototype confirmed blockchain's capacity to secure electoral processes. Votes were immutable once cast, eliminating risks of tampering or deletion. Transparency was enhanced as each vote transaction appeared on the distributed ledger, allowing independent verification by voters and administrators. Voter anonymity was maintained through encryption, while the system successfully flagged and rejected attempts at double voting. Performance tests indicated that the framework handled hundreds of concurrent users with minimal delay, though scalability for millions of voters remains an open issue. Additionally, the system generated cryptographic receipts, enabling voters to confirm inclusion of their ballots in final tallies, thereby improving accountability and trust.

The study's findings align closely with its stated objectives. First, the review of traditional and electronic voting systems confirmed their limitations, particularly inefficiency, lack of transparency, and susceptibility to fraud. Blockchain directly addresses these weaknesses by decentralizing control and embedding immutability in vote records. Second, the exploration of blockchain as a voting framework revealed that its decentralization and cryptographic security significantly enhance transparency, anonymity, and trust, validating its potential for electoral innovation. Third, the analysis of consensus and cryptographic mechanisms emphasized that while PoW is secure, its energy intensity necessitates future reliance on more efficient algorithms such as PoS or PBFT. Finally, the identification of challenges and opportunities highlighted that while blockchain voting is feasible at prototype level, large-scale deployment will require advances in scalability, integration with national databases, legal frameworks, and hybrid models to accommodate offline voters in regions with limited digital infrastructure.

5. Conclusion

Blockchain provides a transformative foundation for secure and transparent e-voting. By ensuring vote immutability, enhancing transparency, and preventing fraud, it strengthens public confidence in electoral processes. Yet, challenges of scalability, inclusivity, and legal adoption remain unresolved. Future research should focus on hybrid online-offline models, energy-efficient consensus protocols, and global standardization frameworks to enable blockchain's widespread electoral deployment.

References

Adekunle, A., & Musa, K. (2023). Biometric innovations in electoral systems: A case study of Ghana and Nigeria. *Journal of African Elections, 22*(1), 56–73.

Ahmed, H. (2017). Conceptual secure blockchain-based electronic voting system. *International Journal of Computer Applications, 165*(2), 1–6.

Alhat, S. (2024). Blockchain and its applications beyond cryptocurrency. *International Journal of Emerging Technologies, 19*(4), 45–59.

AlZain, A., Li, C., & Yang, X. (2024). Security concerns in electronic voting systems. *Computers & Security, 131*, 103–121.

Anita, P., Sharma, R., & Kumar, S. (2020). Cryptographic techniques for verifiable e-voting systems. *Journal of Information Security, 11*(3), 102–118.

Appel, A. (2023). Internet voting: Risks and possibilities. *Communications of the ACM, 66*(9), 32–41.

Ashenfelter, O. (2018). The development of optical scan voting technology. *American Political Science Review, 112*(3), 564–579.

Bartolucci, G., De Nicola, R., Lener, M., & Pedicini, M. (2018). Ethereum-based e-voting using circle shuffle registration. *Future Internet, 10*(5), 53–67.

Benaloh, J., Byrne, M., & Neff, C. (2013). End-to-end verifiable voting systems: Helios and Scantegrity. *IEEE Security & Privacy, 11*(5), 59–67.

Crosby, M., Nachiappan, P., & Verma, P. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation Review, 2*, 6–19.

Debant, A., & Hirschi, L. (2023). Traditional and electronic voting: Costs and benefits. *Journal of Political Technology, 12*(4), 201–218.

Diamond, P. (2023). Blockchain challenges and opportunities in governance. *Journal of Digital Policy, 9*(2), 120–134.

Effah, J., & Debrah, E. (2018). Biometric verification in African elections. *African Journal of Political Science, 12*(2), 45–61.

Fajri, F., Setiawan, A., & Hasibuan, Z. (2020a). Decentralized e-voting using Ethereum blockchain. *International Journal of Computer Science, 17*(3), 99–110.

Fischer, J., Hsu, H., & Smith, J. (2016). Democracy and voting technologies. *Government Information Quarterly, 33*(2), 256–263.

Gottfried, C. P., Achmad, B. M., & Rina, R. (2020). Blockchain-based e-voting systems: A global review. *Journal of Information Technology & Politics, 17*(2), 210–230.

Herron, M., & Sekhon, J. (2003). Overvotes, undervotes, and representation: The 2000 U.S. election. *Political Science Quarterly, 118*(4), 507–527.

Hoy, M. (2017). An introduction to blockchain and its applications in governance. *Library Hi Tech, 35*(4), 584–596.

Huang, Y., Zhang, Y., & Wu, X. (2021). Blockchain-based voting systems: Benefits, challenges, and taxonomy. *Information Systems Frontiers, 23*(3), 567–582.

Jafar, H. M., Saleh, S., & Mohammed, A. (2021). Challenges in blockchain-based voting: A review. *Journal of Internet Technology, 22*(4), 755–769.

Kamal, A., Ahmed, B., & Iqbal, M. (2023a). Blockchain for election security and transparency. *Journal of Information Security, 12*(1), 15–28.

Kamal, D., Disha, G., & Rudresh, P. (2023b). Framework for blockchain-based e-voting in developing countries. *International Journal of E-Governance, 9*(2), 80–95.

Kolvenbach, S., Ruland, M., & Gräther, W. (2018). Blockchain in education and certification. *International Journal of Information Management, 39*, 314–321.

Kushwaha, S., & Singh, R. (2020). Evolution of blockchain technologies. *Journal of Computer Science, 18*(4), 233–245.

Michael, B., Ronald, M., & Patricia, S. (2015). Estonia's i-voting system: Lessons learned. *Government Information Quarterly, 32*(3), 296–301.

Park, C. (2019). Cryptographic receipts and transparency in voting. *Journal of Cryptographic Engineering, 9*(2), 101–115.

Pawlak, M., Krasuski, M., & Kowalski, P. (2021). Security and privacy issues in blockchain e-voting. *Journal of Cybersecurity, 7*(1), 23–35.

Popper, N. (2015). *Digital gold: Bitcoin and the inside story of the misfits and millionaires*. Harper.

Quoc, H., & Quang, N. (2018). Blockchain technology for future advancement. *International Journal of Computer Science, 15*(2), 77–89.

Salem, S. M. K., Ali, M. E. E., Abdulmawla, M. A. N., & Mohamed Abd, A. M. Z. (2023b). A blockchain e-voting framework for Libya. *Journal of Governance and Innovation, 7*(1), 99–114.

Schroeder, R. (2016). Big data and the risk to privacy in elections. *Information, Communication & Society, 19*(2), 178–195.

Shneider, C. (2017). Transparency in elections: Paper ballots vs. electronic systems. *Journal of Electoral Studies, 25*(3), 189–202.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.

Tapscott, D., & Tapscott, A. (2017). *Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world*. Penguin.

Verma, P., Srivastava, R. D., & Kumar, S. (2024). Consensus mechanisms in blockchain applications. *Journal of Distributed Systems, 15*(1), 88–101.