International Journal of Advancing Research, Innovation and Entrepreneurship

Vol 1(3), DOI:10.82036/6hebpv04, December 2025 *ISSN: 2977-9332*

Blockchain-Based Voting System for Enhanced Election Security

[*1]Bashir Abubakar, [2]Nurudeen Mahmud Ibrahim, [3]Kayode Ibrahim Adenuga

[1,2] Faculty of Computing, Nile University of Nigeria, Abuja

[3]University of Law Business School, Birmingham, United Kingdom

[3]Centre for Research, Innovation, Development and Entrepreneurship (CRIDE), United Kingdom

*Corresponding Author Email address: abubakarmbashir@gmail.com

ABSTRACT

The reliability of electoral systems is essential to democratic integrity, yet traditional voting methods often face issues like tampering, impersonation, and lack of transparency. This research proposes a block chain-based voting system to enhance trust, security, and transparency. Built on the Polygon network for scalability and low cost, the system uses SHA-256 to anonymize voter identities and smart contracts to enforce one-person-one-vote logic. Unique Identification Number (NIN) verification ensures only eligible voters participate. Each vote is immutably recorded, eliminating manual counting and enabling real-time result computation. The system demonstrates strong performance, resilience to threats, and cost-efficiency, offering a scalable solution for secure digital elections.

Keywords: Cyber security, E-voting, Election Security, Block chain, Smart Contract

1 INTRODUCTION

The integrity of elections is fundamental to democracy, yet traditional systems, whether paper-based or electronic face persistent threats, including fraud, manipulation, and lack of transparency (Kohno et al., 2004; Kersting & Baldersheim, 2004). Across the globe, these issues have undermined public trust and cast doubt on democratic outcomes (Jafar et al., 2021; Ndakaripa, 2020).

Blockchain technology has emerged as a promising solution, offering verifiable, immutable, and decentralized record-keeping (Johnson, 2019; Peelam et al., 2024). Voting systems have evolved from paper to electronic to online voting (Nemes et al., 2021). Paper-based systems are vulnerable to tampering and logistical inefficiencies (Willemson, 2018), while electronic and online methods often suffer from software vulnerabilities and lack of end-to-end verifiability (Mazri, 2023; Dabhi et al., 2024). Blockchain offers a paradigm shift through decentralized consensus, immutability, and verifiability (Dong et al., 2024). Each vote is treated as a cryptographically secured, time-stamped transaction, resistant to post-election tampering (Peelam et al., 2024). Cryptographic hashing and consensus mechanisms further strengthen system resilience (Rani et al., 2024).

Several countries have piloted blockchain voting: Estonia, Zug (Switzerland), Sierra Leone, India, Utah (USA), South Korea, Japan, and Australia, with varying success and challenges (Babickaitė, 2024; Košt'ál et al., 2019; Specter et al., 2020). Brazil and Russia have also explored blockchain to improve electoral transparency (Jafar et al., 2021).

Standards from NIST and the U.S. EAC recommend end-to-end encryption, biometric and multi-factor authentication, cryptographic integrity checks, and blockchain auditability as best practices for secure voting systems. Despite its promise, blockchain voting faces unresolved issues: scalability, voter anonymity vs. transparency, high implementation costs, and legal/regulatory uncertainty. Public awareness and trust in technology are also critical for adoption.

This research contributes a practical, secure blockchain voting model tailored to Nigeria's electoral landscape. By combining national ID verification with blockchain transparency and automation, it seeks to advance democratic integrity through resilient and verifiable electoral processes. This study addresses critical issues such as ballot tampering, impersonation, and limited auditability, which collectively erode electoral credibility (Ogala & Oneh, 2024; Onu & Uche, 2020). By leveraging blockchain's decentralized architecture and cryptographic security, the proposed system enhances transparency, integrity, and accessibility (Alsunaidi et al., 2024). It integrates Nigeria's National Identification Number (NIN) system for voter authentication and license-based verification to ensure only eligible citizens can vote (Kumar et al., 2023).

The research aims to: (1) assess limitations of current voting systems, (2) design a secure blockchain-based architecture, (3) implement smart contracts for eligibility enforcement and automated tallying, and (4) evaluate the system's performance using a prototype deployed on the Polygon network (Wicaksana et al., 2024; Benedetti & Henry, 2024).

Vol 1(3), DOI:10.82036/6hebpv04, December 2025 ISSN: 2977-9332

2 RELATED WORKS

Several countries have experimented with blockchain-based voting systems, providing valuable insights. Estonia integrated blockchain into its national e-voting system, ensuring transparent and tamper-proof records, positioning itself as a digital governance leader (Kshetri & Voas, 2018). In Zug, Switzerland, a blockchain referendum trial preserved voter anonymity while enabling public auditability (Babickaitė, 2024). Sierra Leone's 2018 election partnered with Agora to explore blockchain's role in enhancing transparency, particularly in developing nations (Košťál et al., 2019). India piloted blockchain voting in Telangana and Andhra Pradesh using biometric authentication, showing its potential for secure remote voting in large democracies (Kumar et al., 2023). Utah conducted a mobile blockchain voting trial for overseas military personnel, emphasizing accessibility without compromising transparency (Specter et al., 2020). South Korea's K-Voting system facilitated secure local elections, although scaling it nationally remains a challenge (Mannonov & Myeong, 2024). Japan's Tsukuba integrated blockchain with national ID for secure municipal elections (Taş & Tanrıöver, 2020). Horizon State in Australia used blockchain in corporate and community settings to improve trust in organizational voting (More et al., 2021). Brazil applied blockchain to secure election results (Jafar et al., 2021), and Russia piloted blockchain voting in Moscow's municipal elections to enhance trust, though some security issues persisted (Suwito et al., 2021).

In parallel, industry standards play a crucial role in shaping secure voting systems. The National Institute of Standards and Technology (NIST) provides robust security frameworks, including access controls, auditing, and risk assessments, while the U.S. Election Assistance Commission (EAC) promotes Voluntary Voting System Guidelines (VVSG) to ensure system integrity, privacy, and accessibility. Key security mechanisms recommended include end-to-end encryption for secure data transmission, biometric and multi-factor authentication for identity verification, cryptographic integrity checks to prevent vote manipulation, and blockchain auditability for public verification without compromising voter privacy.

Despite the promise of blockchain in voting, several challenges persist in the literature. Scalability remains a critical limitation, as processing millions of transactions in real-time without compromising performance is still unresolved. Maintaining voter anonymity while ensuring transparency presents a paradox, particularly on public blockchains. Techniques such as zero-knowledge proof or privacy-preserving protocols require further exploration. The complexity and cost of implementation, especially in low-resource regions, are often underestimated. Moreover, public perception, adoption willingness, and understanding of blockchain systems remain largely unexamined, which can hinder trust and widespread acceptance. Legal and regulatory uncertainties also add complexity, with little clarity around jurisdiction, data protection, and cross-border election standards.

By addressing these gaps and building on prior implementations, this study contributes to the ongoing discourse on secure, verifiable, and inclusive voting technologies, offering a practical model tailored to Nigeria's electoral needs. The proposed system demonstrates how blockchain, when aligned with best practices and national identification systems, can uphold democratic values through secure and transparent voting.

3 METHODOLOGY

A prototype voting platform was developed on the Polygon network with a layered architecture: a React/TypeScript frontend, Express.js backend, PostgreSQL (Supabase) for off-chain data, and smart contracts for on-chain voting. Voter authentication used Nigeria's National Identification Number (NIN), with each vote recorded immutably via blockchain. The system prioritized security using the STRIDE and DREAD models. Mitigations included multi-factor authentication, end-to-end encryption, digital signatures, access controls, and Sybil attack prevention through strict NIN verification. Distributed architecture and rate-limiting defended against DoS attacks.

Security testing combined automated (MythX, Slither) and manual penetration tests were conducted to evaluate vulnerabilities in smart contracts and authentication flows. Data for evaluation came from system logs and feedback from voters, election officials, and developers. Surveys and interviews explored usability, trust, and administrative efficiency. Logs tracked metrics like transaction times, gas costs, and error rates. Qualitative data underwent thematic analysis, while quantitative data were analyzed statistically, including performance scaling and significance tests.

Ethical standards were upheld through informed consent, data anonymization, and secure data storage. The research emphasized transparency by sharing findings with participants. The architecture supported a modular, scalable, and secure voting platform, balancing off-chain efficiency with on-chain integrity. The findings affirm the system's potential for secure, transparent, and scalable electronic voting.

4 KEY IMPLEMENTATION FEATURES

4.1 VOTER REGISTRATION

The voter registration process in the proposed blockchain-based voting system of Figure 1 ensures security and data integrity through a structured flow. It starts with the user entering their National Identity Number (NIN), which is validated based on country-specific rules. The system then checks for a connected blockchain wallet (for example, MetaMask or Phantom). Once both NIN and wallet are verified, the data is submitted to the backend, where checks are performed to prevent duplicate registrations. If unique, the entry is stored with an "unverified" status pending admin review. A confirmation message is then sent to the user with instructions for the next steps. This process incorporates validation, error handling,

Vol 1(3), DOI:10.82036/6hebpv04, December 2025 ISSN: 2977-9332

and security to ensure a smooth and reliable registration experience.

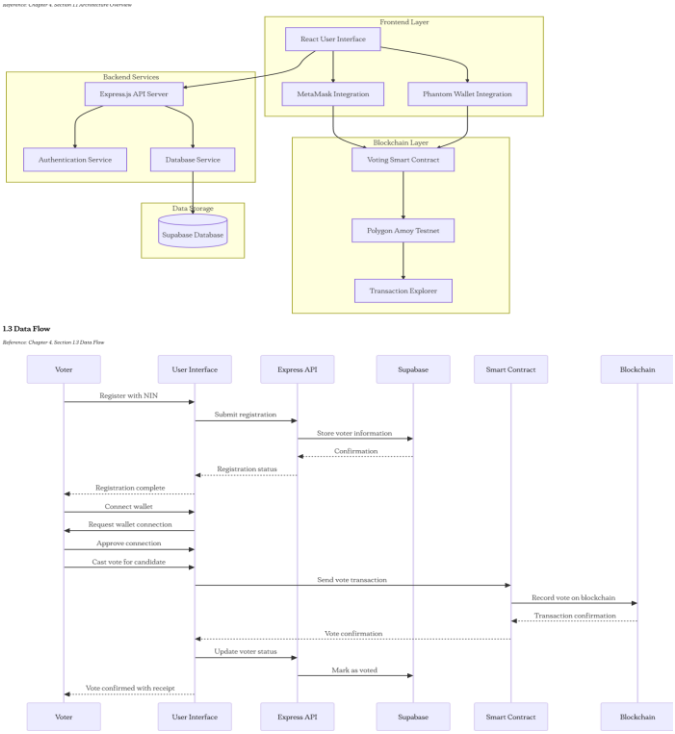


Figure 1: System Architecture

4.2 Vote Casting Process

The vote casting process in the proposed blockchain-based voting system is designed to be secure, transparent, and tamper-proof; Figure 2 displays the vote casting process. It begins with the voter selecting a preferred candidate in the active election and initiating the vote by clicking the "Cast Vote" button. To protect voter identity and ensure anonymity, the system hashes the voter's National Identity Number (NIN) using SHA-256, which also helps prevent duplicate voting. The system then prompts the user to connect a blockchain wallet, such as MetaMask or Phantom, and approve the transaction. Before proceeding, a duplicate check is performed to verify that the voter has not already voted in the current election. If eligible, the system creates a blockchain transaction, executes the smart contract to record the Election ID, Candidate ID, and Voter Hash, digitally signs the transaction, and broadcasts it to the blockchain network where it is validated and stored immutably. Upon successful confirmation, the voter's status is updated to prevent double voting, and a transaction receipt with a hash is provided as verifiable proof of voting. The system also includes pre-submission validations, real-time error notifications, and automatic retries to handle common issues like insufficient funds or network congestion, ensuring a smooth and secure voting experience.

4.3 Blockchain Vote Recording Mechanism

The blockchain recording process in the proposed voting system guarantees the integrity, transparency, and immutability of every vote. The system interacts with the Voting System smart contract deployed on the Polygon Amoy testnet, enabling decentralized and tamper-proof vote storage. Communication between the frontend and blockchain is handled through Web3.js and Ethers.js, which facilitate secure wallet interactions and transaction signing. Each vote transaction includes the Election ID, Candidate Index, and a SHA-256 hashed NIN to ensure voter anonymity. Prior to confirmation, estimated gas fees are displayed, and the voter must approve the transaction via their wallet. Once confirmed, the transaction is signed with the voter's private key and broadcast to the blockchain. To prevent double voting, the system disables the vote button post-submission, verifies voter uniqueness through hashed NIN in the smart contract, and updates voter status in an off-chain database. After successful recording, a receipt is generated containing the transaction hash, block number, timestamp, and candidate information ensuring transparency without compromising voter privacy. This process upholds the security, reliability, and auditability of the voting system.

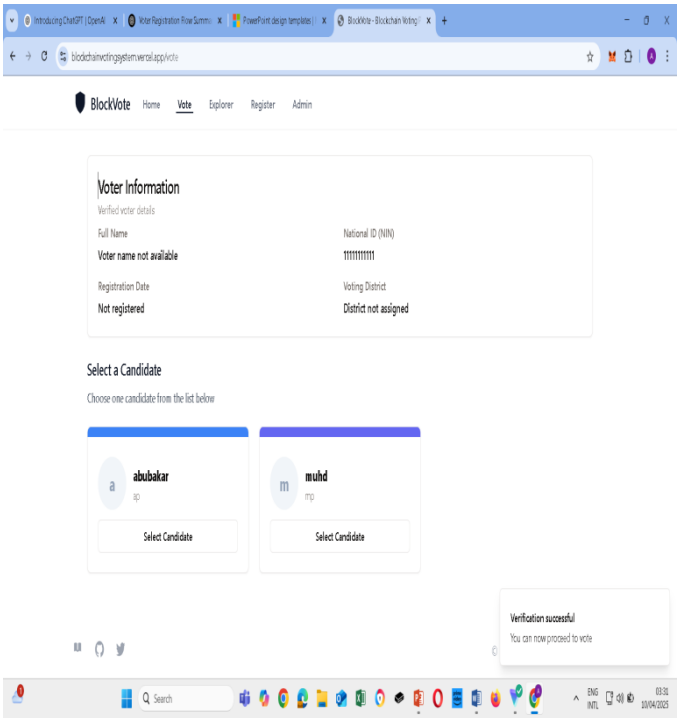


Figure 2: Voting Page (Candidate selection)

4.4 Anonymity and Privacy Mechanisms

The voting system employs a multi-layered privacy protection framework to safeguard voter anonymity while ensuring election integrity. Identity protection is achieved through SHA-256 cryptographic hashing of National Identity Numbers (NINs), producing irreversible hashes prefixed with

Vol 1(3), DOI:10.82036/6hebpv04, December 2025 ISSN: 2977-9332

"0x" to match blockchain formatting standards. This allows the system to detect duplicates without revealing actual identities. Only hashed NINs are stored on chain, serving as pseudonymous identifiers to prevent traceability. A strict data segregation strategy is enforced voter identities and voting records are stored separately, with no database containing both elements. The blockchain ledger holds vote records without personal identifiers, and the off-chain database maintains verification status only. Privacy is further enhanced through Web3 wallet integration, which ensures users retain control of their private keys, and through secure HTTPS communication and role-based access control. Additionally, off-chain records are automatically purged after election completion to minimize data exposure. These mechanisms collectively uphold voter privacy, build trust and support a secure and anonymous voting experience.

5 SYSTEM EVALUATION

The Block Vote system underwent a rigorous multi-layered testing approach, comprising unit testing, integration testing, and end-to-end (E2E) testing, where unit tests verified smart contract logic, hash function reliability, UI responsiveness, and form validation; integration tests ensured seamless interaction among the frontend, backend, blockchain, and database through smart contract deployment, API validations, and synchronization checks; and end-to-end tests simulated full user journeys including voter registration, admin election management, vote casting with wallet confirmation, and transaction receipt validation, all executed within an isolated test environment using tools like Cypress and mocked Web3 providers to ensure functionality, security, and usability across the entire BlockVote ecosystem, and following the tests, several issues were identified and resolved, such as fixing double voting prevention in smart contracts, correcting election time miscalculations, strengthening admin access control, resolving frontend wallet connection inconsistencies, enhancing form validation, fixing mobile UI bugs, optimizing blockchain event listeners for transaction confirmation, implementing retry logic for database sync failures, and standardizing API error responses—thus ensuring a robust, secure, and user-friendly final deployment.

6 CONCLUSION

The proposed blockchain-based voting system enhances electoral integrity by leveraging the Polygon network for scalability and cost-effectiveness. Utilizing SHA-256 hashing ensures voter anonymity, while smart contracts enforce a strict one-person-one-vote policy. Integration with Nigeria's National Identification Number (NIN) system ensures that only eligible voters can participate. Each vote is immutably recorded on the blockchain, facilitating real-time result computation and eliminating the need for manual counting. This system demonstrates strong performance, resilience to threats, and cost-efficiency, offering a scalable solution for secure digital elections.

7 REFERENCES

Achieng, M., & Ruhode, E. (2013). The adoption and challenges of electronic voting technologies within the South African context. arXiv preprint arXiv:1312.2406.

Alsunaidi, S. J., Aljamaan, H., & Hammoudeh, M. (2024). MultiTagging: A Vulnerable Smart Contract Labeling and Evaluation Framework. Electronics, 13(23), 4616.

Bedford, S. (2021). The 2020 presidential election in Belarus: Erosion of authoritarian stability and re-politicization of society. Nationalities Papers, 49(5), 808–819.

Benarous, L., & Boudjit, S. (2024). Blockchain-Based Privacy-Aware Voting System. SN Computer Science, 5(8), 1079.

Benedetti, A., Henry, T., & Tucci-Piergiovanni, S. (2024, March). A Comparative Gas Cost Analysis of Proxy and Diamond Patterns in EVM Blockchains for Trusted Smart Contract Engineering. In International Conference on Financial Cryptography and Data Security (pp. 207–221). Springer Nature Switzerland.

Dong, S., Su, H., Hou, R., & Shankar, A. (2024). Improved PBFT Consensus Mechanism Based on Voting Sort Clustering Partition With Group Signature for IoT. IEEE Transactions on Intelligent Transportation Systems.

Fabrega, A., Fábrega, J., Orsini, S., & Torres, M. (2024). Protecting voter privacy in decentralized voting systems. Journal of Cryptography and Information Security, 16(4), 112–128.

Herbawi, O., & Husini, M. (2023). Hybrid Voting System. International Journal of Political Technology, 18(2), 44–59.

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—review and open research challenges. Sensors, 21(17), 5874.

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. Sensors, 21(17), 5874.

Johnson, D. (2019). Blockchain-based voting in the US and EU constitutional orders: A digital technology to secure democratic values? European Journal of Risk Regulation, 10(2), 330–358.

Kersting, N., & Baldersheim, H. (2004). Electronic voting and democracy: A comparative analysis. Palgrave Macmillan.

Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004, May). Analysis of an electronic voting system. In IEEE Symposium on Security and Privacy, 2004. Proceedings (pp. 27–40). IEEE.

Košťál, K., Bencel, R., Ries, M., & Kotuliak, I. (2019, October). Blockchain e-voting done right: Privacy and transparency with public blockchain. In 2019 IEEE 10th

Vol 1(3), DOI:10.82036/6hebpv04, December 2025 ISSN: 2977-9332

International Conference on Software Engineering and Service Science (ICSESS) (pp. 592-595). IEEE.

Kumar, G., Yadav, S. S., Singh, R., & Mittal, A. (2023, November). Electronic Voting System Using Blockchain. In International Conference on Innovations in Data Analytics (pp. 77-87). Singapore: Springer Nature Singapore.

Kumar, G., Yadav, S. S., Singh, R., & Mittal, A. (2023, November). Electronic Voting System Using Blockchain. In International Conference on Innovations in Data Analytics (pp. 77–87). Springer Nature Singapore.

Mannonov, K. M. U., & Myeong, S. (2024). Citizens' Perception of Blockchain-Based E-Voting Systems: Focusing on TAM. Sustainability, 16(11), 4387.

Mazri, T., & Krissi, G. (2023, October). Electronic Voting: Review and Challenges. In The Proceedings of the International Conference on Smart City Applications (pp. 110–119). Springer Nature Switzerland.

More, M. P., Patil, M. D., & Patil, M. N. (2021). Blockchain Based E-Voting System.

Ndakaripa, M. (2020). Zimbabwe's 2018 elections: Funding, public resources and vote buying. Review of African Political Economy, 47(164), 301–312.

Nemes, M., Schwerdt, R., Achenbach, D., Löwe, B., & Müller-Quade, J. (2021). And Paper-Based is Better? Towards Comparability of Classic and Cryptographic Voting Schemes. Cryptology ePrint Archive.

Nikolaevich, L. S. (2022). Electronic Voting: New Opportunities or Challenges for Democracy. Скиф. Вопросы студенческой науки, 11(75), 330–336.

Ogala, E., & Oneh, O. G. (2024). Development of an online voting system in cloud computing environment. Journal of Software Engineering and Applications, 2(3).

Onu, F. U., & Uche, W. E. (2020). Analysis of the Strengths and Weaknesses of Online Voting Systems: The Way Forward. IOSR Journal of Computer Engineering, 22(2), 53–57.

Peelam, M. S., Kumar, G., Shah, K., & Chamola, V. (2024). DemocracyGuard: Blockchain-based secure voting framework for digital democracy. Expert Systems, e13694.

Rani, M. A. H. C., Jamil, M., & Kamalulai, A. A. (2024). Exploring the Impact of Bitcoin as a New Form of Property on the Maqasid Shariah: Maslahah and Mafsadah Perspective. Islamic Finance and Blockchain Studies.

Specter, M. A., Koppel, J., & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in {US}. federal elections. In 29th USENIX Security Symposium (USENIX Security 20) (pp. 1535-1553).

Suwito, M. H., Ueshige, Y., & Sakurai, K. (2021). Evolution of Bulletin Board & its application to E-Voting–A survey. Cryptology ePrint Archive.

Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. Symmetry, 12(8), 1328.

Wicaksana, A., Widjaja, M., & Marcellino, M. (2024, November). Scalability Evaluation of zk-SNARK Authentication in Blockchain-Based E-Voting. In 2024 Joint 13th International Conference on Soft Computing and Intelligent Systems and 25th International Symposium on Advanced Intelligent Systems (SCIS&ISIS) (pp. 1–5). IEEE