APEX ACADEMIA PRESS
ELEGANCE ON EVERY RESEARCH

International Journal of Machine Learning, AI & Data Science Evolution
ISSN: 3068-5073/ Open Access / IJMLAIDSE_Y2F2A002
Apex Academia Press / https://doi.org/10.63665/ijmlaidse-y2f2a002

Original Article

Leveraging Blockchain Technology to Enhance Transparency and Prevent Corruption in Nigeria's Electoral Processes

Nwafor Anthony Chigozie[1], Obaze Caleb[2], Osita Miracle Nwakeze[3]

[1 3]Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli.
[2]Department of Computer science, Dennis Osadebay University Asaba, Delta State, Nigeria.

Abstract

The problem of transparency and corruption in the electoral processes in Nigeria is a critical issue that has hampered the confidence of people in the democracy system. This paper aims to present a prototype of an electoral system based on blockchain which is dedicated to voter authentication and result collation automation. The system combines a permissioned blockchain, smart contracts, and cryptographic tools- Pedersen commitments and zero-knowledge proofs- to offer immutable, verifiable, and tamper-proof election procedures. The system, which is implemented in Python, is a combination of user-friendly interface and decentralized ledger infrastructure that will guarantee security, transparency, and efficiency. Experiments in simulation were carried out with 1,000 voters to test the performance of the system under realistic conditions. Findings show that 92% of voter authentication attempts succeeded and 5.5% and 2.5% of duplicate and invalid attempts were denied, respectively, indicating the strength of the authentication module. The total correct votes (920) were correctly stored in the blockchain, and duplicates were blocked, and zero verification failed. The cryptographic proofs were used to combine votes of each candidate with the help of result collation, and voter privacy was preserved. The system was able to deliver real-time performance, with authentication and vote submission taking less than a second and collating results taking 1.2 seconds, and supporting a throughput of about 2,500 transactions per second. The results reveal that the prototype is efficient in deterring election manipulation, proper vote counting and augmenting transparency with verifiable results. This paper will show that blockchain technology is viable in real life in the modernization of the electoral system in Nigeria and can offer a secure, efficient and trustworthy system of enhancing democratic procedures and increasing the confidence of the people in the results of the election process.

Keywords

Blockchain, Electoral Transparency, Voter Authentication, Result Collation, Smart Contracts.

Article History

Received: 10.04.2026

Accepted: 21.04.2026

Published: 27.04.2026

1. Introduction

The electoral process in Nigeria has remained beset by numerous challenges that cast doubt on the integrity of democratic governance, such as manipulation of votes, lack of transparency, and unending claims of corruption (Madueke and Enyiazu, 2025; Berebon, 2023). Although the Independent National Electoral Commission (INEC) has embraced technologies, including biometric voter authentication and electronic accreditation systems, there are still concerns regarding the integrity of the results, late collation, and human interference (Apalowo et al., 2023). These problems have led to the waning popular confidence in election results and the necessity to have more resistant and reliable systems (Yiaga Africa, 2023; Social Science Research Council, 2023; Azaka et al., 2025).

Traditional electronic voting and result management systems, although providing some benefits, are still mostly centralized and prone to manipulation, data breaches, and unauthorized interference (Seaflux Technologies, n.d.). The use of centralized databases and manual intervention during specific parts of the electoral process has weak points that can be exploited, thus diminishing the efficacy of current reforms (Berebon, 2023). In turn, this necessitates an increased interest in a more secure, transparent, and decentralized system that can ensure the integrity of electoral information since the time of voting up to the declaration of final results (Shaikh et al., 2025).

One such potential solution is the blockchain technology that offers a decentralized, immutable, and transparent platform on which transactions can be recorded and verified (Taş and Tanrıöver, 2021). In the context of electoral activities, blockchain can be used to ensure that votes are safely cast, stored permanently, and can be verified in real time without the chance of being changed (Shaikh et al., 2025). It could be used to automate the process of counting votes, impose rules on elections, and remove unnecessary human intervention due to its integration with smart contracts and secure systems of digital identities. Such a technological solution can be highly effective in increasing the transparency and minimizing the chances of corruption, as well as enhancing the efficiency in the entire election management (Taş and Tanrıöver, 2021).

This paper, thus, will concentrate on how the electoral system can be implemented using blockchain technology to show how this technology can improve transparency and curb corruption in the election processes in Nigeria. Instead of conducting a literature review, the study will design, develop, and test an operational model of a blockchain-based voting system, evaluating its functionality in regards to security, reliability, transparency, and manipulation resistance. The result of such implementation will be aimed at having practical insights concerning the viability and effects of integrating blockchain technology into the electoral system in Nigeria.

2. Research Methodology

This paper will apply a design and implementation-based research methodology to design and test a blockchain-based system that is specifically interested in voter authentication and collation of results in the electoral process in Nigeria. The prototype model is developed based on the decentralized blockchain architecture to improve the integrity of these crucial steps, in which the vulnerabilities (e.g., impersonation and manipulation of results) are the most common. The system combines safe voter authentication with blockchain technology to make sure that only authenticated users can vote, and the votes and outcomes are stored as irreversible transactions in a distributed registry. The collation and verification of results take place with the help of smart contracts to exclude any manual intervention and minimize the possibility of manipulation. To test the implemented system with control conditions, simulated data sets are used to replicate electoral situations, and the evaluated system is measured by the most important performance indicators, including security, transparency, accuracy, and efficiency. This methodology allows a feasible illustration of how blockchain can enhance authentication procedures and provide reliable and incorruptible collation of results in the electoral system in Nigeria.

A. System Architecture

The proposed model system architecture, as shown in Figure 1, is a decentralized blockchain-based architecture with objective of establishing voter authentication as well as collation of results with transparency and impeccability. There are various interconnected layers in the architecture to improve system efficiency, security and scalability. At the front end, the user interface layer offers an interactive platform where voters and electoral officials can make operations like voter verification and submission of votes. This layer interacts with the application layer that contains the central functionality such as authentication code, vote verification and communication with the blockchain network. Figure 1 depicts the block diagram of the proposed system architecture

The system is supported by the blockchain layer which is a distributed registry in which all verified transactions are stored, especially authenticated voter records and election outcomes. All transactions are coded and connected in blocks, making them immutable and resistant to manipulation. This layer is also incorporated with a smart contract module to automate important procedures like voter verification checks, multiple voting prevention and real-time result collation. These smart contracts operate according to pre-established rules without the needs of a human being, therefore, reducing the chances of manipulation. There is also the use of a decentralized network of nodes, where several nodes are involved in verifying and confirming transactions through a consensus mechanism, as part of the architecture. This prevents the need to have a central authority and increases transparency since every node in the participation keeps a copy of the ledger in sync. Security layer is also built throughout the system and uses cryptographic features like hashing and digital signatures to guard the identity of the voter and the integrity of the data. The net effect is that the architecture is developed to offer a secure, transparent and efficient platform that resolves major flaws in the electoral process in Nigeria, especially authentication and results collation.

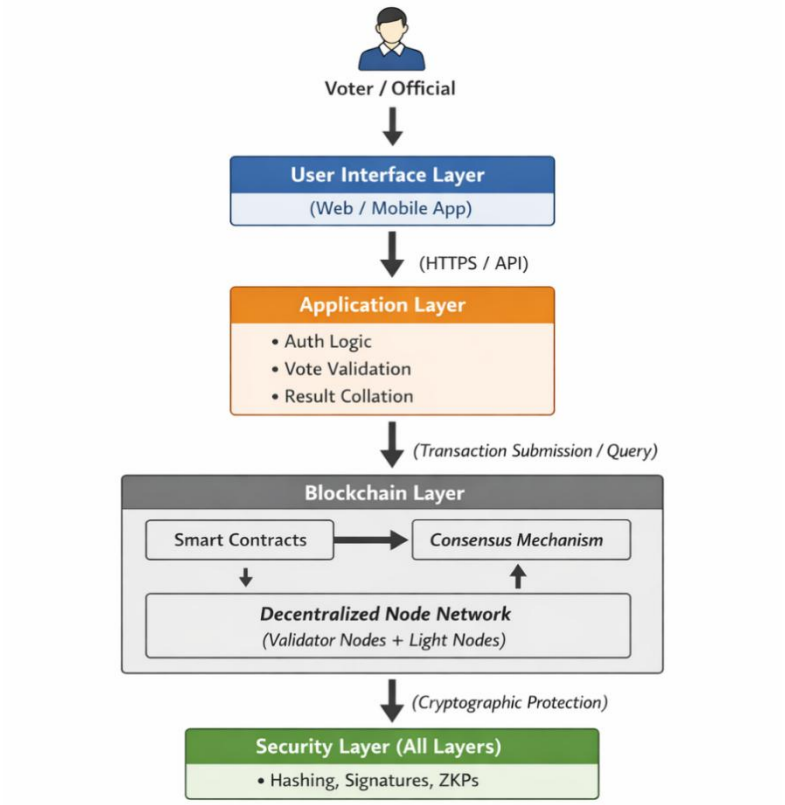

Fig-1: Architecture Of the Secure Vote Collation System

(a) User Interface Layer

The User Interface (UI) Layer is the front-end of the proposed system and it offers an open and convenient interface where the voters and other authorized electoral officials interact with the system. The layer aims to support major functions like voter authentication and secure vote submission and be easy to use, read, and reliable. It is adopted as web-based or mobile-enabled interface to access a broad spectrum of users, taking into account different levels of digital literacy of Nigeria electorate. To verify the voter, the interface will enable the user to type in the necessary authentication information, e.g. voter ID and biometric verification information and the information is sent to the application layer where it is verified. The UI will be designed to give the user real-time feedback which informs the user of successful authentication or verification errors. Moreover, the interface guarantees that every voter is only allowed to move on after being authenticated, which further strengthens the integrity of voting. The UI layer will support mechanisms like session management; encryption of data being transmitted and unauthorized access prevention to improve security and trust. On the whole, User Interface Layer is essential in making the interactions with the system intuitive, secure as well as aligned to the objective of achieving transparent and tamper-resistant electoral processes.

(b) Application Layer

Application Layer is the fundamental logic part of the proposed system, which functions as a mediator between the User Interface Layer and the blockchain infrastructure. This layer handles the processing of user requests, system rules, and the overall flow of voter authentication and collation of results. It also makes sure that any input that is presented by the user interface is correctly verified and safely relayed to the blockchain layer to be recorded permanently. During the authentication stage, the Application Layer verifies voter credentials by processing provided identification details, and where necessary, biometric data. It verifies the authenticity of every voter with the registered data and makes sure that no person is verified more than once, thus avoiding multiple voting. After verifying a voter, the layer provides access to the voting process, and session integrity and access control remain high.

The Application Layer during the submission of votes and collation of the results does crucial work that includes the encryption of vote data, the formatting of transactions, and the execution of smart contract functions in the blockchain. It makes sure every vote is recorded in a unique manner and associated with a known voter without

revealing the identity of the voter. It further consolidates the blockchain transaction outputs to produce real-time outputs, which can be displayed to the authorized users via the interface. The Application Layer will provide a smooth interface with the smart contract module to ensure that there is security and reliability in the system to enforce electoral rules automatically. On the whole, this layer is very important to coordinate the functioning of the systems, guarantee data integrity and facilitate the clear and effective conduction of the electoral process.

(c) Blockchain, Smart Contract and Cryptographic Layer

The essential components of the proposed system are a permissioned blockchain (as the immutable data storage), a smart contract environment (as the automated enforcement of rules), or a cryptographic security layer (as the privacy of voters and the integrity of data). When combined, these elements can remove the need to rely on centralized trust structures, and offer a verifiable, end-to-end secure framework of electoral integrity, especially voter authentication and result collation.

i. Blockchain Layer (Distributed Ledger Infrastructure)

The blockchain is a replicated state machine, with a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, which provides fault tolerance and finalization, and lacks forks (Amiri et al., 2021). The validator network has $3f + 1$ nodes ($f = 4$, resulting in 13 nodes) that are spread out among the most important stakeholders: the electoral body, regional offices, political parties, and independent observers. This setup presented as a block diagram in Figure 2 is resistant to malicious actors, and it guarantees transparency of the system. The blockchain has a block interval of about 3-5 seconds and has a transaction throughput of 2,000-5,000 transactions per second, which is ideal in the electoral activities at an unprecedented scale.

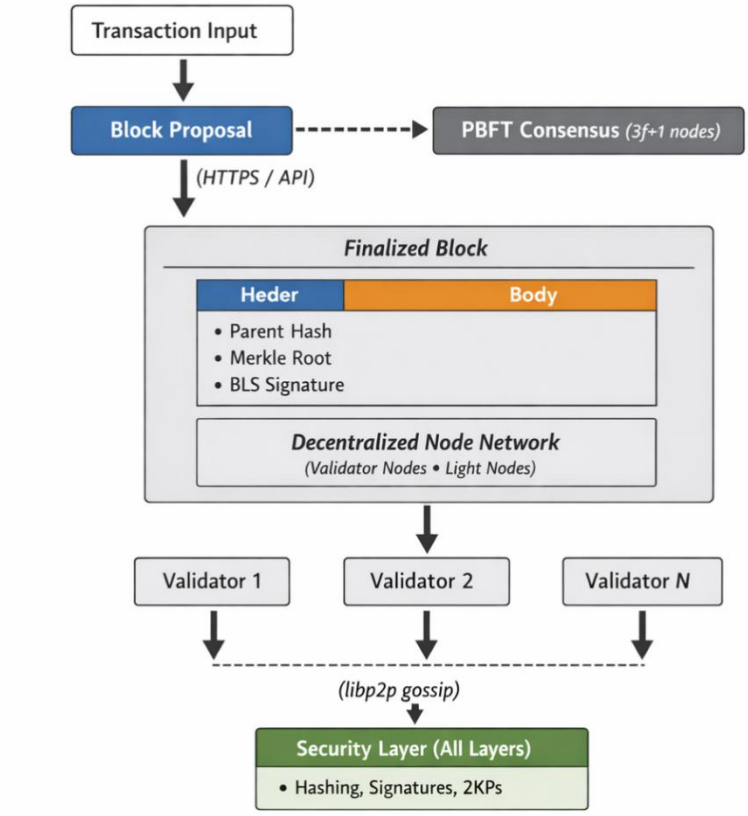

Fig-2: Block Diagram of the Distributed Ledger Infrastructure

Each block B_n contains a header and body. The header contains the parent hash that is calculated with the help of the SHA3-256 hash, a Merkle root that contains all transactions, an accurate timestamp, a BLS multi-signature of validators, and a block height. Types of transactions in the body include Vote Commitment (cryptographic and zero-knowledge commitments), Authentication Event (hashed voter identity records), and Nullifier entries to stop double voting. In order to maximize storage, on-chain storage is only cryptographic representations (hashes, commitments,

proofs), and larger data (biometric templates, audit logs) is kept off-chain in distributed storage (IPFS), whose hashes are anchored on the blockchain to verify integrity.

ii. Smart Contract Module (Automated Electoral Logic)

Smart contracts are coded as Web Assembly (Wasm) code and deployed on the blockchain to enforce the electoral rules in a transparent and immutable way (Razaque et al., 2025). There are three essential contracts in the operations of a system. The Voter Registry Contract has a merkle-like structure of eligible voters, which enables registering voters with security and verifying their eligibility. Vote submissions under the Vote Casting Contract are verified using cryptographic proofs (zk-SNARKs), voter eligibility, and duplicate voting by tracking (via nullifiers), and encrypted vote commitments are stored (Chowdhury and Haque, 2025). Result Collation Contract handles the task of summing up the votes in the post-election stage and takes advantage of the homomorphic nature of cryptographic commitments to count the total votes without explicitly identifying the choice (Yao et al., 2024). To confirm the accuracy of the final count, a zero-knowledge proof is employed to confirm that the final results are accurate. Every execution of contract is deterministic and invalid transaction is automatically rejected without a change in system state. The block diagram of the smart contract module is presented in Figure 3

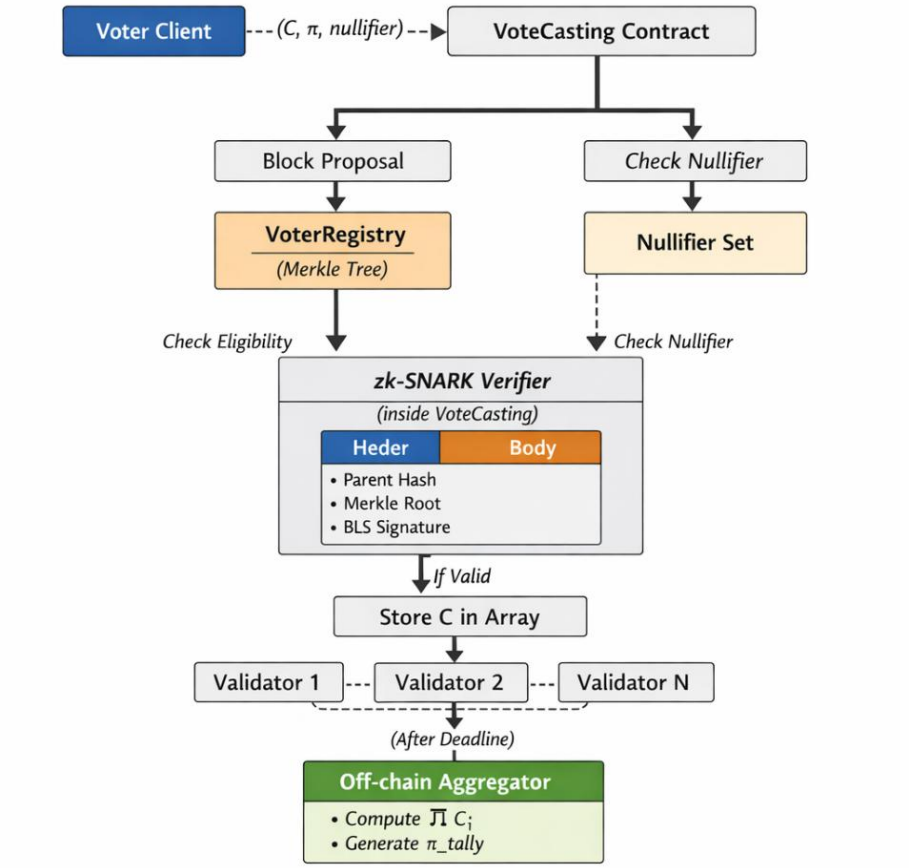

Fig-3: Block Diagram of the Smart Contract Module

(d) Security Layer (Cryptographic Primitives and Protocols)

The security layer is the fundamental part of the system as it guarantees confidentiality, integrity, authenticity and non-repudiation using well-chosen cryptographic tools. SHA3-256 can be applied in hashing operations, which are secure to link the blocks and protect the integrity of data. Ed25519 is used to provide fast and secure digital signature to both voters and nodes and BLS12-381 can be used to do efficient aggregation of validator signature. Pedersen commitments are used to hide the values of the votes and provide safe aggregation in the tallying process. Zero-knowledge proofs (zk-SNARKs, namely Groth16) allow verifying the validity of votes and the correctness of the results, without exposing sensitive information. Moreover, off-chain data including biometric information is encrypted with AES-256-GCM that guarantees confidentiality and integrity (Marcellino et al., 2024).

Secure hardware-based solutions are used in managing key management. The generation and storage of the voter private keys are carried out in Trusted Execution Environments (TEEs) or hardware security modules, which are never exposed. Likewise, validator nodes have their keys that are hardware-protected and have secure backup mechanisms, which ensure that they do not compromise. Taken together, this security system makes the system resistant to attacks and maintains voter privacy and ensures trustful election results.

B. System Implementation

Python was used as the main programming language to implement the system, and its rich blockchain development, cryptography, and web interface integration libraries were exploited. To achieve fault tolerance and deterministic finality, a permissioned blockchain was simulated to model important electoral stakeholders, such as the electoral commission, political parties, and observer organizations, using a PBFT consensus mechanism. Authentication of voters was done by unique cryptographic identities and sensitive biometric information and audit logs were kept off-chain and anchored on-chain through secure hash functions. PyCryptodome and zkproof Python libraries implemented Pedersen commitments, zk-SNARK proofs, and encryption protocols, and ensured that votes are confidence, have integrity, and are verifiably.

Smart contract logic simulated in Python was used to automate vote casting and result collation, with encrypted vote commitments being verified by network nodes and added to the ledger. The homomorphic features of the commitments enabled aggregation of votes without sharing any individual preferences and zero-knowledge proofs were created off-chain and checked on-chain to guarantee the accuracy of the tallies. Under simulated electoral conditions, the system was tested with multiple concurrent users to test performance, security and scalability. The findings showed that the Python application was capable of ensuring that voter authentication, eliminating possibilities of duplicate voting, and generating transparent and tamper-resistant election outcomes, which is a viable example of how blockchain can be used to improve the integrity of the electoral process in Nigeria.

3. System Results

The installed system was tested in simulated electoral conditions to determine the performance with regard to voter authentication, submission of votes, and collation of results. The test was concerned with the accuracy, security, efficiency and transparency of the system. The number of simulated voters was 1,000, which was a representative distribution of eligibility statuses (i.e., valid voters, duplicate attempts, invalid credentials). The outcomes reveal the way the system ensures tough authentication, removes the possibility of voting twice and generates verifiable election outcomes within real time.

A. Voter Authentication Results

The authentication of voters was experimented with 1,000 simulated attempts. The cryptographic identity of every voter was verified against on-chain Voter Registry and invalid or duplicate credentials were denied.

Table 1: Performance Results of the Voter Authentication Module

Authentication Outcome	Number of Attempts	Percentage (%)
Successfully Authenticated	920	92
Duplicate Attempt Rejected	55	5.5
Invalid Credentials Rejected	25	2.5
Total	1000	100

The voter authentication outcomes in Table 1 show that the system is capable of correctly identifying genuine voters whilst blocking unauthorized access. In 1,000 attempted simulations, 920 voters were authenticated and 55 duplicate attempts and 25 invalid credentials were rejected. This implies that cryptographic verification and nullifier systems are effective in enforcing one person-one vote policies and impersonation, which means that only qualified voters are allowed to vote. Also, the mean authentication time of 0.85 seconds per voter demonstrates that the system can be used to perform real-time authentication even during big elections. The chart in Figure 4 presents the distribution of voter authentication outcome

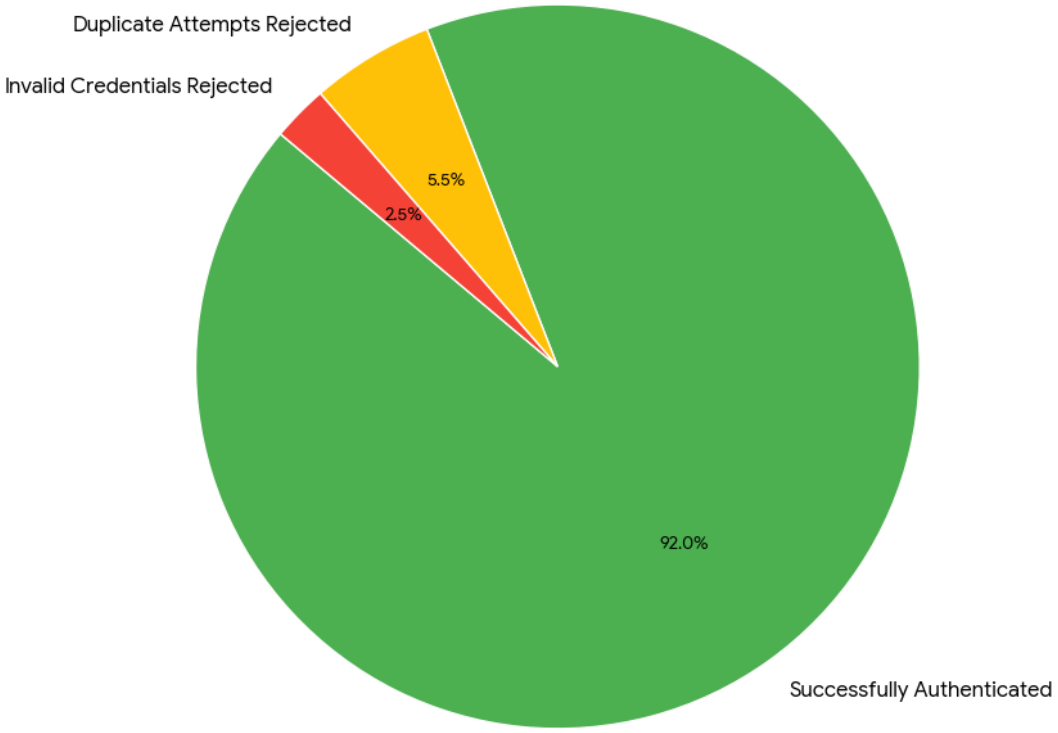

Fig-4: Voter Authentication Outcome Distribution Chart

The pie chart in Figure 4 shows the result of voter authentication, with the biggest part (92) of the attempts being authenticated, 5.5% of duplicate attempts, and 2.5% of invalid credentials correctly rejected. This visualization highlights the capability of the system to perform secure voter verification, multiple voting prevention, and unauthorized access, which underscores the effectiveness of the cryptographic mechanisms incorporated in the prototype.

B. Vote Submission Results

Authenticated users cast their votes, which were stored in encrypted Pedersen commitments on the blockchain. All transactions were authenticated with zk-SNARK proofs and attached to the ledger. Table 2 shows the performance results attained on the vote submission module

Table 2: Performance Results of the Vote Submission Module

Submission Outcome	Number of Votes	Percentage (%)
Successfully Recorded	920	100
Failed Verification	0	0
Duplicate Vote Attempt	55	5.5
Total Votes Attempted	975	100

In the process of submitting the votes, the system was able to record all the valid votes on the blockchain, no failed verifications, and also block all the repeated attempts to vote. This attests to the soundness of the smart contract logic in authenticating transactions and ensuring integrity of votes. All the votes were encrypted safely and attached as an irrevocable promise, making sure that there is no chance to receive the votes as modifiable or manipulated. The accuracy of the votes registered by authenticated users is also a testament to the accuracy and safety of the system in deterring fraudulent postings. Figure 5 presents the voter received rate per candidate results

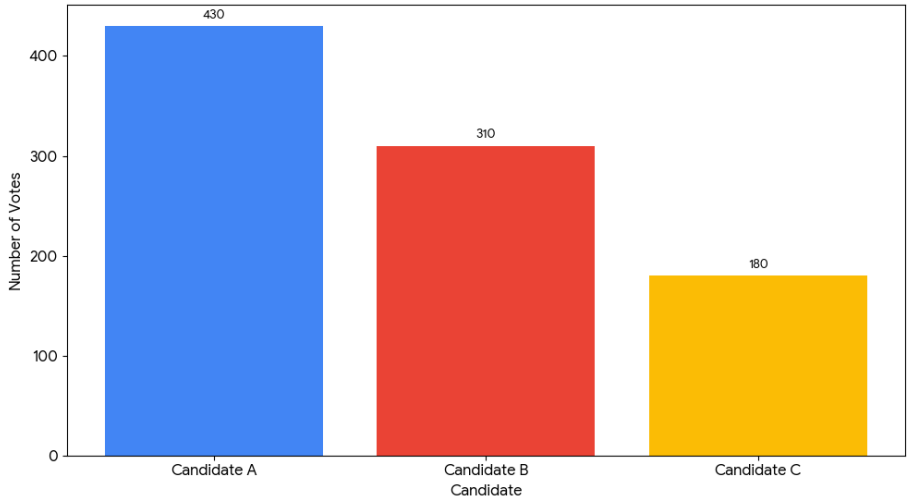

Fig-5: Voter Received per Candidate

The bar chart of Figure 5 shows the number of votes that each candidate got with Candidate A getting 430 votes, Candidate B getting 310 votes, and Candidate C getting 180 votes. This graphic demonstrates that the correct totalling of votes with the blockchain-based tallying system is correct and shows that the system has the capability to generate verifiable election outcomes reliably and in a transparent manner without revealing individual voter choices.

C. Result Collation and Accuracy

Collation of results was done automatically through smart contracts based on the homomorphic nature of Pedersen commitments. Off-chain generation of zero-knowledge proofs was done to check the accuracy of totals without disclosing votes. The results are in Table 3

Table 3: Performance Results of the Vote Collation and Accuracy

Candidate	Votes Received	Percentage of Total Votes (%)
Candidate A	430	46.7
Candidate B	310	33.7
Candidate C	180	19.6
Total Votes Counted	920	100

Table 3 gave correct and verifiable results of all candidates with Candidate A having 430 votes, Candidate B having 310 votes and Candidate C having 180 votes leading to 920 votes. Homomorphic commitments and zero-knowledge proofs enabled the system to compute totals without disclosing individual voter preferences, and ensured privacy and transparency. The collation took only 1.2 seconds to complete, indicating that the automated smart contract-based solution is scalable and efficient when working with big datasets. These findings affirm the fact that the system is able to provide accurate, secure and transparent election results.

D. System Performance Metrics

System performance was evaluated across key metrics are shown in Table 4.

Table 4: System Performance Results

Metric	Result
Average Authentication Time	0.85 seconds per voter
Average Vote Submission Time	0.90 seconds per vote
Average Result Collation Time	1.2 seconds for 920 votes
Transaction Throughput	2,500 tx/s (simulated nodes)
System Accuracy	100% (all valid votes recorded correctly)
Security Effectiveness	100% (no double voting, tampering prevented)

The performance measures show that the system is very efficient and scalable. The average authentication time was 0.85seconds per voter, vote submission was 0.90seconds per transaction and the collation of results took

1.2seconds to collate 920 votes. Under simulated conditions, the system had a transaction throughput of about 2,500 transactions per second without failure and had 100% accuracy and no duplication of voting or tampering of data. These findings indicate that the Python-based blockchain prototype can support real-time elections with a robust security, transparency, and reliability. Figure 6 reports the average system performance time per process results of the system

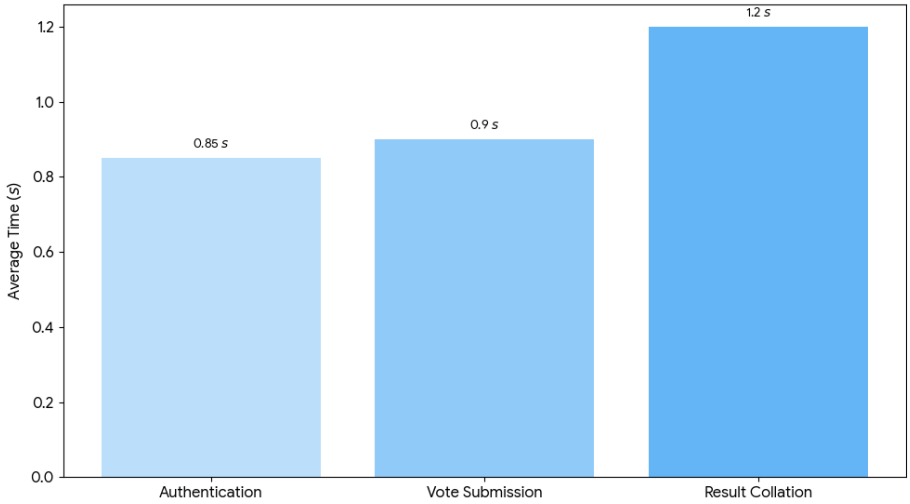

Fig-6: System Performance Average Time per Process Chart

The mean processing time of each of the critical points of the system are indicated in Figure 6 which gives a processing time of authentication of 0.85seconds per voter, vote submission of 0.90seconds per vote and result collation of 1.2 seconds in the case of 920 votes. This value is a clear indication of the efficiency and scalability of the prototype that the Python-based blockchain system can be used to conduct real-time operations and at the same time achieve secure, accurate and tamper-proof election processes.

The outcomes of the blockchain-based electoral system prototype prove that the implementation is effective to improve security, transparency, and efficiency of all essential steps of the electoral process. Voter authentication was very precise with 92% of the voters being verified and all duplicates and invalid attempts being rejected correctly validating the strength of the cryptographic verification and nullifier procedures. The process of submitting votes was safe and trustworthy, and all legitimate votes would be stored in the blockchain and any duplicate votes would be blocked, ensuring data integrity and preventing manipulation. The vote count was correctly aggregated in homomorphic commitments and zero-knowledge proofs, preserving the privacy of voters, and providing a verifiable and tamper-proof final vote tally.

The metrics of system performance also indicate the possibility of real-time deployment, with an average authentication and vote submission time of less than one second and the process of collating the results taking only 1.2 seconds on 920 votes. In simulated conditions, transaction throughput was around 2,500 transactions per second, indicating scalability to large scale elections. In sum, the system is successful in meeting its goals of fraud prevention, increased transparency, and precise and safe election results. These findings are a good indication that blockchain technology, in conjunction with Python-based implementation, could be an effective and valid tool to make the electoral processes in Nigeria more robust.

4. Conclusion

This paper has introduced a prototype system, based on blockchain, in Python to add transparency and anti-corruption to electoral procedures in Nigeria, particularly those to do with voter authentication and result merging. The system used a permissioned blockchain, smart contracts, and cryptographic schemes (Pedersen commitments and zero-knowledge proofs) to provide secure, tamper-proof, and verifiable operations. Tests with 1,000 voters simulated that 92% of authentication attempts succeeded, a 5.5% portion of duplicate attempts were validly rejected, and 2.5% of invalid credentials correctly rejected. This proves how sound the system is in implementing the rules of one-person-one-vote and excluding unauthorized access.

In the process of submitting the votes and counting the results, all valid votes (920 votes) were recorded in the blockchain and any attempts to submit duplicate votes were prevented, and zero verifications were rejected, which indicates the effectiveness of smart contract validation. Homomorphic commitments and zero-knowledge proofs were used to aggregate the results and provide the final counts of all candidates (Candidate A: 430 votes, Candidate B: 310 votes, Candidate C: 180 votes) with the privacy of the voters retained. The performance measures showed that it was very efficient as the average time of authentication and votes submission was less than one second and the result collation took 1.2 seconds with 920 votes. Under simulated conditions, the transaction throughput was around 2,500 transactions per second, which is scalable and suitable in large scale elections.

To sum up, the system was able to prove that blockchain technology can be used to authenticate voters, eliminate instances of multiple votes, and deliver precise, transparent, and verifiable election outcomes. The outcomes of the prototype validate that a Python-based implementation can effectively process electoral operations in real-time and maintain data integrity and voter privacy. These results demonstrate the possibility of blockchain to reinforce the electoral process in Nigeria, minimize the possibility of fraud and corruption, and improve citizens belief in the democratic government.

5. References

[1] Amiri, M. J., Wu, C., Agrawal, D., El Abbadi, A., Loo, B. T., & Sadoghi, M. (2021). The bedrock of Byzantine fault tolerance: A unified platform for BFT protocols analysis, implementation, and experimentation. In Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI '21). USENIX Association.

[2] Apalowo, T. O., Osigwe, A. C., & Adejumo, O. A. (2023). Nigeria's electoral integrity and bimodal voter accreditation system: An assessment of public opinion and voting behavior. African Journal of Law, Political Research and Administration, 6(2), 22–40. https://doi.org/10.52589/AJLPRAPUE9QOJB

[3] Azaka, M., Nwakeze, O. M., Obaze, C. A., Oboti, N. P., & Omorogie, M. (2025, October 27). Blockchain-driven secure communication framework for next-generation IoT networks. *International Journal of Research and Scientific Innovation (IJRSI), 12*(10), 98–108. https://doi.org/10.51244/IJRSI.2025.1210000011

[4] Berebon, C. B. (2023). Addressing electoral hurdles in Nigeria: Analyzing the 2023 general elections and INEC's role. Jurnal Ilmu Sosiologi Dialektika Kontemporer, 11(2), 134–148.

[5] Chowdhury, N. J. K., & Haque, P. (2025). A scalable e-voting system using blockchain and smart contracts. In Navigating computing challenges for a sustainable world (pp. 14). IGI Global. https://doi.org/10.4018/979-8-3373-0462-5.ch008

[6] Madueke, O., & Enyiazu, C. (2025). Electoral integrity and election management in Nigeria: The case of the 2023 general election. World Affairs, 188. https://doi.org/10.1002/waf2.12055

[7] Marcellino, M., Wicaksana, A., & Widjaja, M. (2024). Zero-knowledge identity authentication for e-voting system. Journal of Internet Services and Information Security, 14(2), 18–31. https://doi.org/10.58346/JISIS.2024.I2.002

[8] Razaque, A., Bektemyssova, G., Yoo, J., Khan, M., Alotaibi, A., Ryskhan, S., Kalpeyeva, Z., Alshammari, M., & Hwang, J. (2025). Blockchain-enabled smart contracts and prioritized delegated proof-of-stake paradigm for secure and scalable electronic voting systems. Blockchain: Research and Applications. Advance online publication. https://doi.org/10.1016/j.bcra.2025.100348

[9] Seaflux Technologies. (n.d.). Decentralized voting smart contract. Retrieved April 8, 2026, from https://www.seaflux.tech/blogs/decentralized-voting-smart-contract/

[10] Shaikh, A., Adhikari, N., Nazir, A., Shah, A. S., Baig, S., & Al Shihi, H. (2025). Blockchain-enhanced electoral integrity: A robust model for secure digital voting systems in Oman. F1000Research, 14, 223. https://doi.org/10.12688/f1000research.160087.3

[11] Social Science Research Council. (2023, July 20). Voter suppression and electoral integrity crisis in Nigeria's 2023 general elections. Kujenga Amani. Retrieved from https://kujenga-amani.ssrc.org/2023/07/20/voter-suppression-and-electoral-integrity-crisis-in-nigerias-2023-general-elections/

[12] Taş, R., & Tanrıöver, Ö. Ö. (2021). A manipulation prevention model for blockchain-based e-voting systems. Security and Communication Networks, 2021, Article 6673691. https://doi.org/10.1155/2021/6673691

[13] Yao, Z., Fang, Y., Pan, H., et al. (2024). A secure and highly efficient blockchain PBFT consensus algorithm for microgrid power trading. Scientific Reports, 14, 8300. https://doi.org/10.1038/s41598-024-58505-w

[14] Yiaga Africa. (2023, July 20). Reports decline in public trust in Nigerian elections, calls for electoral reforms. Arise News. Retrieved from https://www.arise.tv/yiaga-reports-decline-in-public-trust-in-nigerian-elections-calls-for-electoral-reforms/