International Journal of Cyberspace Security

https://journals.cypedia.net/ijcs

ARTICLE

Design and Threat Modeling of a Permissioned Blockchain Voting System for Resource-Constrained Democracies: A Case Study of Nigeria

Prince Onebieni Ana [1] ***, Nonye Emmanuael Maidoh*** [2] ***, Augustine Chidiebere Onuora*** [2*] ***, Obiora Emeka Ikedilo*** [2] ***, Anthony Obogo Otiko*** [1] ***, Joseph Osahon Idemduia*** [2] ***, Favour Uzoh Umennakenyi*** [2] ***, Ogbonna Umeh Inya*** [2]

[1] *Computer Science Department, University of Cross River, Calabar P.M.B. 1123, Nigeria*

[2] *Computer Science Department, Akanu Ibiam Federal Polytechnic Unwana, Unwana P.M.B. 1007, Nigeria*

ABSTRACT

This paper presents the design and threat modeling of a permissioned blockchain voting system tailored for resource-constrained democracies, using Nigeria as a case study. We propose a hybrid on-chain/off-chain architecture based on Proof of Authority (PoA) consensus to ensure energy efficiency, scalability, and civic accountability in low-connectivity environments that stores vote hashes, vote timestamps, and validator signatures on-chain while keeping biometric metadata and device logs off-chain using decentralized storage to reduce bandwidth. The framework integrates Nigeria's National Identity Management Commission (NIMC) biometric database for cryptographic voter verification and employs smart contracts to automate vote validation. A STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege)-based threat model is applied to identify risks such as spoofing, tampering, and denial-of-service attacks, repudiation, information disclosure, and elevation of privilege in politically volatile contexts. Unlike existing blockchain voting models developed for high-capacity states, this system is context-aware, designed for 40% internet penetration, infrastructural instability, and institutional distrust. The study adopts Design Science Research (DSR) methodology to build, demonstrate, and evaluate the artifact. We validate the system's feasibility by simulating network degradation and threat scenario injection on a

*CORRESPONDING AUTHOR:

Augustine Chidiebere Onuora, Computer Science Department, Akanu Ibiam Federal Polytechnic Unwana, Unwana P.M.B. 1007, Nigeria; Email: holyaustin@yahoo.com

ARTICLE INFO

Received: 2 October 2025 | Revised: 6 November 2025 | Accepted: 14 November 2025 | Published Online: 22 November 2025
DOI: https://doi.org/10.64797/ijcs.v1i2.110

CITATION

Ana, P.O., Maidoh, N.E., Onuora, A.C., et al., 2025. Design and Threat Modeling of a Permissioned Blockchain Voting System for Resource-Constrained Democracies: A Case Study of Nigeria. International Journal of Cyberspace Security. 1(2): 1–12.
DOI: https://doi.org/10.64797/ijcs.v1i2.110

Hyperledger Fabric testnet. Using Design Science Research (DSR), we built a Hyperledger Fabric testnet with 10 validator nodes and simulated 500 votes under 10–80% connectivity. Findings show that a locally governed, hybrid blockchain model can enhance electoral integrity while remaining feasible in developing democracies. This work contributes to the digital democracy discourse by introducing a context-aware, legally grounded blockchain voting model for low-connectivity democracies.
Keywords: Blockchain Voting; Permissioned Ledger; Proof of Authority; Threat Modeling; Electoral Integrity; Biometric; Design Science Research; Hyperledger Fabric

1. Introduction

In many developing democracies, elections remain a paradox—routinely conducted but rarely trusted[1]. Nigeria, which is the largest democracy in Africa, has suffered a lot of election crises, from vote buying, logistic failures, rigging, to post-election violence, which has actually made the populace lose faith in the entire election process[2]. The 2023 election was marred with technical glitches, delay of results and allegations of result manipulation even after the huge expenditure on reforms like purchase and use of biometric, voter registration, smart card reader and the Bimodal Voter Accreditation System (BVAS)[3].

An emerging technology such as the Blockchain technology can help restore hope and trust in Nigeria's electoral system as it is known for its immutability, decentralization, and real-time auditability as opposed to the centralized server, which can be easily manipulated[4,5]. But countries like Estonia or Switzerland that have used the blockchain for their electoral process have stable internet, high digital literacy, and institutional neutrality, unlike most African countries[6].

It is with displeasure that we state that about 40% of the population of Nigeria remains offline and politicians benefit from electoral opacity; this makes the blockchain voting model unfit and not feasible[7]. Research on locally governed, safe, and context-aware blockchain voting systems for politically fragile and low internet connectivity locations is severely lacking.

We are proposing a permissioned blockchain voting framework specifically designed for Nigeria's infrastructural and institutional realities in this paper. We are bringing in three key innovations:

1. A hybrid on-chain/off-chain architecture that can operate under intermittent connection.
2. Legal-code coupling, where smart contracts enforce provisions of the Electoral Act 2022.
3. A multi-stakeholder Proof of Authority (PoA) consensus model involving the Independent National Electoral Commission (INEC), judiciary, civil society, and party agents as validators—ensuring civic oversight.

While recent studies propose blockchain for African elections (e.g., Essex et al.[8]; Arhin Jnr et al.[9]), none integrate legal-code coupling with multi-stakeholder PoA under real-world connectivity constraints. This work is the first to co-design a blockchain voting system with Nigeria's Electoral Act 2022 and NIMC infrastructure as core design constraints.

The study adopts Design Science Research (DSR) methodology to build and evaluate the system artifact. A STRIDE-based threat model is applied to assess security in high-risk environments.

This work contributes to the growing field of digital democracy in the Global South by demonstrating how blockchain can be adapted—not imported—to serve sovereign, inclusive, and resilient electoral systems.

2. Related Work

Blockchain-based voting has been explored in several jurisdictions, but with mixed outcomes. Estonia's i-Voting system, while not fully blockchain-based, uses distributed ledger technology to secure audit trails, demonstrating the value of integrated digital identity and long-term e-governance investment[10]. However, its success relies on near-universal broadband and high public trust conditions not replicable in Nigeria.

Sierra Leone's Agora pilot was criticized for a lack of local audit trails and opaque smart contract code, undermining transparency despite blockchain claims[11]. Similarly, West Virginia's trial was halted after researchers demonstrated that mobile devices could be compromised via malware to alter votes without detection[12].

The use of Electronic Voting Machines (EVMs) by India

indicated that non-blockchain digital tools can enhance electoral integrity if they are gradually embraced and approved by the political establishment [13]. Brazil's automated system emphasizes transparency and public education as key to digital trust [14].

The majority of blockchain voting research ignores socio-technical alignment in favor of techno-utopian ideas [15]. Much of the literature on blockchain voting in developing nations suffers from 'techno-solutionism'—assuming technology alone can fix institutional failure [9]. This paper rejects that assumption by embedding the system within Nigeria's legal, political, and infrastructural realities.

Blockchain smart contracts present flexibility and custom programs to decentralized applications (Dapps), but they are faced with usability and performance limitations that enable the research of system-supported transactions to increase acceptance and efficiency [16,17].

All these reviewed models fail to address the unique challenges of low internet connectivity, political volatility, and lack of trust in electoral institutions in African democracies. In this paper, we try to bridge the gap by proposing a context-sensitive hybrid, and legally incorporated blockchain system.

3. Design of the Permissioned Blockchain Voting System

3.1. System Architecture Overview

The suggested approach uses a hybrid architecture, storing critical data such as device metadata, biometric logs off-chain in safe, auditable databases and important data such as vote hashes, timestamps, and validator signatures on-chain (**Figure 1**). This lowers bandwidth requirements and permits asynchronous synchronization in the event of network failures, which is essential for polling units in remote areas with unstable connectivity.

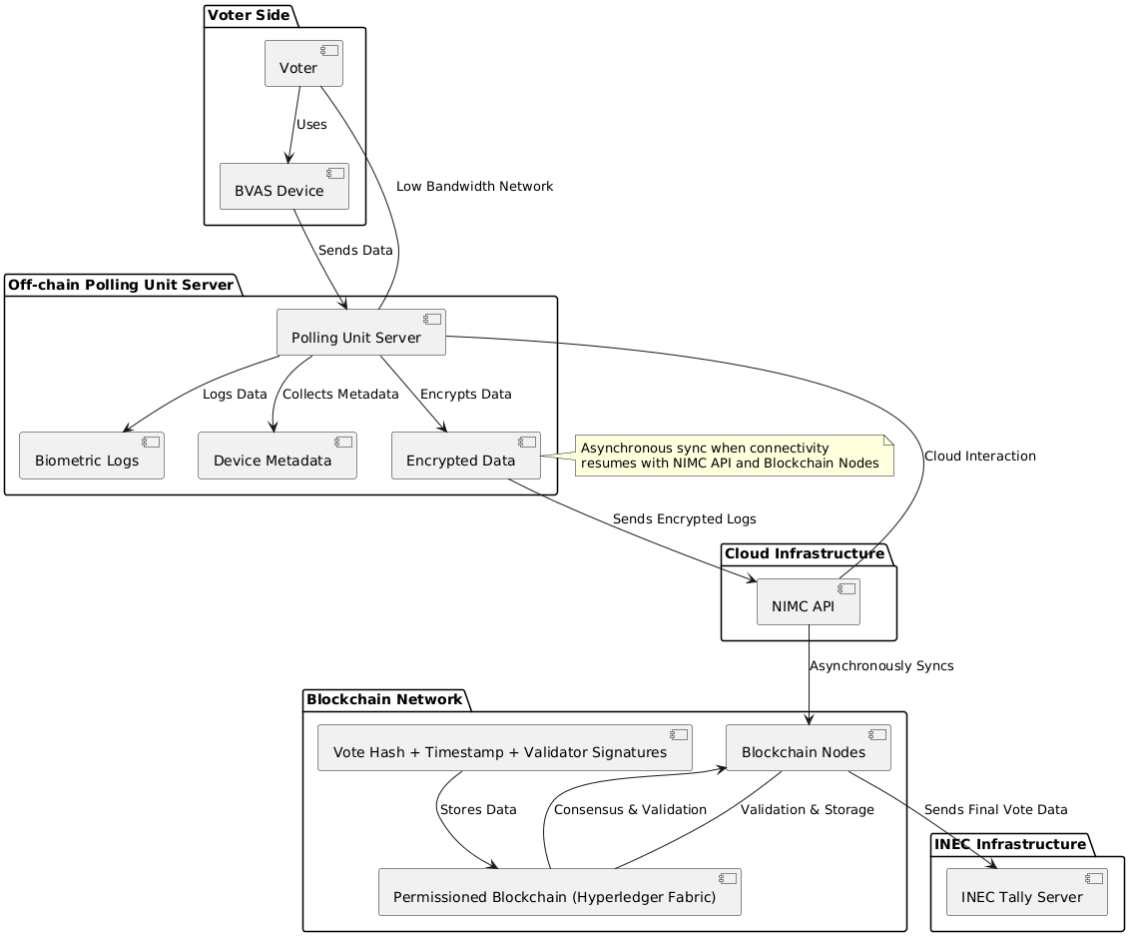

Figure 1. Hybrid On-Chain/Off-Chain Architecture for Nigeria's Resource-Constrained Voting Environment.

3.2. Blockchain Consensus Mechanism: Proof of Authority (PoA)

The Proof of Authority (PoA) is the consensus mechanism that we are proposing in this project, replacing the energy-hungry Proof of Work (PoW) mechanism and wealth-biased Proof of Stake (PoS). Proof of Authority (PoA) depends on a permissioned network of pre-verified validators responsible for transaction validation.

Validators can include:

- Officials of the Independent National Electoral Commission (INEC);
- Judicial representatives;
- Civil society observers (e.g., YIAGA Africa);
- Agents of a political party;
- Representatives of the cybersecurity agency.

Every validator is supposed to run a node that produces blocks. For consensus to be reached, greater or equal to 67% must agree, thereby ensuring resilience against collusion.

Advantages for Nigeria:

- Energy-efficient: Proof of Authority consensus consumes negligible electricity compared to Proof of Work. A single PoA node can run on a Raspberry Pi 4 of 5–10 watts, making it suitable for polling units with solar or unstable grid power. In contrast, Bitcoin-style PoW consensus would require megawatts and is infeasible in rural Nigeria.
- Fast finality: PoA blocks are produced every 5 s, and finality (irreversibility) is achieved once ≥67% of validators (two-thirds of validators) sign. This allows real-time result computation—a political necessity to reduce post-election tension.
- Accountable: Validators are known public stakeholders like INEC officials, judges, party agents or elections observers (civil society). Their identities are disclosed, and they are legally liable under the Electoral Act 2022 for any misconduct. This accountability is absent in permissionless blockchains.
- Governance-aligned: By distributing validator roles across five different institutional types (electoral commission, judiciary, civil society, political parties, cybersecurity agency), we prevent any single entity from controlling the ledger. This aligns with Nigeria's federal character principle and builds multi-party trust.

To get this implemented, the PoA architecture was enforced in the Hyperledger Fabric v2.5, where validators are pre-approved stakeholders with auditable identities[18]. In accordance with Nigeria's four-year electoral cycle, validators are rotated after each state-level election cycle to prevent capture.

However, rotating validators alone does not eliminate centralization risks. Permissioned PoA systems remain vulnerable to cartel formation—if a majority of validators coordinate (e.g., through political patronage or coercion), they can censor votes or fork the ledger. To mitigate this without abandoning energy efficiency, our design includes:

1. Supermajority threshold of 67% (not 51%) to raise collusion cost;
2. Public validator identity disclosure with legal liability for misconduct under the Electoral Act 2022;
3. Automatic node replacement if any validator fails to sign blocks for >30 min, triggering a backup from an alternate list of pre-vetted civil society organizations. These measures balance decentralization, accountability, and feasibility in resource-constrained settings.

3.3. Smart Contracts for Legal-Code Coupling

Smart contracts are self-executing digital rules that automate electoral procedures. We introduce legal-code coupling—embedding provisions of the Electoral Act 2022 into smart contracts.

Legal-code coupling follows the 'code is law' paradigm in blockchain governance[19], but we adapt it to Nigeria's statutory framework to prevent algorithmic authoritarianism.

```
event ResultTally(uint256[] voteTotals);

modifier onlyAfterPollingClosed() {
require(block.timestamp >= pollingEndTimestamp, "Polling not closed");
_;
}
```

```
function tallyVotes() public onlyAfterPollingClosed {
require(block.timestamp <= resultUploadTimestamp + 7200, "Result not uploaded within 2 hours
(Sec. 50)");
emit ResultTally(voteTotals);
}}
```

Key functions of the algorithm:

- Vote validation: Guarantees that each validated identity casts one vote[20].
- Tallying trigger: After polls close, votes are automatically tallied.
- Results disqualification: According to Section 50 of the Electoral Act, results that are not posted within 2 h are rejected.
- Transparency log: Records all actions on-chain for audit.

This ensures procedural compliance without human discretion, reducing opportunities for manipulation.

3.4. Cryptographic Identity Verification

Voter identity is secured through integration with Nigeria's National Identity Management Commission (NIMC) database. Each voter's biometric data (fingerprint, facial scan) is hashed and stored on-chain as a digital identity token.

To preserve voter anonymity while ensuring uniqueness, we use a commitment scheme where voter identity is hashed using SHA (Secure Hash Algorithm)-3-256 and linked to a non-reversible ZK-SNARK (Zero-Knowledge Succinct Non-interactive Argument of Knowledge) proof[17]. This allows verification without exposing biometrics on-chain. Future work will implement full ZK-Rollups to meet Nigeria's Data Protection Act (NDPA) requirements.

During voting:

1. Voter authenticates via a BVAS-like device.
2. System verifies hash against NIMC ledger.
3. Voter casts an encrypted ballot.
4. The vote is recorded as an anonymous transaction.

This prevents duplicate registration and ghost voting while preserving anonymity[17].

4. Threat Modeling Using STRIDE Framework

To evaluate security in politically volatile environments, we apply the STRIDE threat model[21], which assesses six categories of digital threats as shown in **Table 1**.

Table 1. STRIDE Threat Model.

Threat	Component	Risk Level	Justification	Mitigation
Spoofing	Voter Identity	High	The NIMC database has been compromised in the past (e.g., 2019 ghost voters); BVAS devices can be cloned	Multi-factor: Biometric + NIMC hash + validator signature
Tampering	Vote Record	Low	Blockchain immutability + ≥67% PoA consensus makes alteration computationally infeasible	PoA + Merkle tree hashing
Repudiation	Vote Submission	Medium	Voter may deny casting vote; no receipt mechanism	Non-revealing receipt: Hash of vote + timestamp signed by validator
Information Disclosure	Vote Privacy	Medium	On-chain vote hashes may be linkable if metadata leaked	Zero-knowledge proofs (future); off-chain encryption
Denial of Service	IReV Sync	High	40% internet penetration + power outages make sync unreliable	Off-chain buffer + batch upload on reconnect
Elevation of Privilege	Validator Node	Medium	INEC or party agent node could be hacked	Role rotation, audit logs, multi-sig for node access

- **DREAD Risk Assessment**

We assign scores (1–10) across five dimensions: Damage, Reproducibility, Exploitability, Affected Users, and Discoverability. DREAD scores (1–10) were assigned by a panel of 3 cybersecurity experts (2 academic, 1 INEC advisor) using NIST SP 800-30 guidelines. Scores reflect Nigeria's context: high collusion risk due to political patronage[22].

- **Elaboration of DREAD Scoring Methodology**

Table 2 holds the rubric used for scoring. The DREAD scores in **Table 3** were assigned by a panel of three cybersecurity experts: two academic researchers with specialization in blockchain security and one advisor to the Information and Communication Technology (ICT) directorate. Each expert independently rated every threat on a scale of 1 (very low) to 10 (very high) for the five DREAD dimensions, following the rubric in **Table 2** (below). The final score for each threat is the arithmetic mean of the five dimension scores, averaged across the three experts.

Table 2. DREAD scoring rubric used by the expert panel.

Dimension	1–3 (Low)	4–6 (Medium)	7–10 (High)
Damage	Minor inconvenience	Disclosure of some voter data	Complete loss of electoral integrity, violence
Reproducibility	Very hard to reproduce	Reproducible with expert knowledge	Easily reproducible (e.g., script kiddie)
Exploitability	Requires physical access/insider	Requires moderate skill or time	Remotely exploitable with low skill
Affected Users	<1% of voters	1–20% of voters	>20% of voters or entire election
Discoverability	Well hidden, no public info	Published but not widely known	Widely known attack (e.g., DDoS tools)

Table 3. DREAD-Based Risk Assessment of the blockchain voting system.

Threat	D	R	E	A	Dsc	Avg	Risk Level	Rationale
Sybil Attack	8	7	6	9	5	7.0	High	Expert panel noted high potential for fake voter identity injection due to weak off-chain identity binding.
DDoS on Sync Module	7	8	7	8	6	7.2	High	Polling units are low-bandwidth and vulnerable to disruption during critical sync windows.
Device Compromise	9	6	8	7	4	6.8	High	BVAS devices are physically accessible in polling stations, increasing the physical attack surface.
Validator Collusion	10	5	4	10	3	6.4	High	Permissioned blockchain has limited validator nodes; collusion could override vote hashes.
Coercion	6	7	6	6	2	5.4	Medium	Voters may be pressured at polling stations; biometric logs cannot detect coercion.
Quantum Attack	10	2	2	10	1	5.0	Medium	Theoretical future threat: We noticed that existing cryptographic primitives like SHA-256 and ECDSA are not quantum-resistant even though quantum attacks are not yet prevalent.

Note: D = Damage, R = Reproducibility, E = Exploitability, A = Affected Users, Dsc = Discoverability.

Detailed scoring rubric and an example calculation are provided in Section 4.

The Risk scores are the arithmetic mean of D, R, E, A, and Dsc.

- **Example—Validator Collusion Score Calculation**

Damage = 10 (collusion can rewrite the ledger, disenfranchise all voters, and cause post-election violence).

Reproducibility = 5 (requires coordination of ≥3 validators, but political patronage makes it plausible).

Exploitability = 4 (attackers need to compromise multiple high-profile individuals, not just a server).

Affected Users = 10 (all voters and the entire electoral outcome).

Discoverability = 3 (collusion would be hidden unless a whistleblower comes forward).

Mean = (10 + 5 + 4 + 10 + 3)/5 = 6.4 → High risk.

This explicit rubric and example make the scoring transparent and repeatable.

5. Methodology: Design Science Research (DSR)

The methodology that we used for this research is the Design Science Research (DSR) methodology [23] because it helps in the creation, demonstration, and evaluation of innovative artifacts used in solving real-world problems. DSR is ideal for technical frameworks in information systems and aligns with these publication standards.

The research follows the six-cycle DSR process:

1. Identification of Problem: Nigeria's electoral system has been suffering from vote rigging, logistical failures, and low public trust. Specifically, the 2023 election saw 28% of BVAS devices fail and 40% of polling units unable to transmit results (Independent National Electoral Commission (INEC) [6]). This creates a need for a tamper-evident, low-connectivity voting system.
2. Objective of Solution: To design a permissioned blockchain voting system that (a) operates reliably at

≤30% internet connectivity, (b) enforces the Electoral Act 2022 automatically via blockchain smart contracts, and (c) provides real-time auditability without requiring high network bandwidth.

3. Design and Development: We built a Hyperledger Fabric v2.5 network with 10 validator nodes, each running on a Raspberry Pi 4 (4 GB RAM). The chaincode (smart contract) implements the legal-code coupling described in Section 3.3. Off-chain buffering uses local SQLite databases that sync when connectivity resumes.
4. Demonstration: The system is illustrated through **Figure 1** (architecture diagram) and the threat models in Section 4. We also provide pseudocode for the tallying smart contract.
5. Evaluation: We evaluated the artifact using (i) STRIDE/DREAD threat modeling with a panel of experts, (ii) a 72-h simulation on a testnet with 500 synthetic votes under 10–80% connectivity, and (iii) a comparative cost analysis against manual voting and BVAS + IReV.
6. Communication: This work will serve as a contribution to knowledge and also serve as the primary communication of this research.

The artifact was evaluated on a Hyperledger Fabric testnet with 10 validator nodes and 500 simulated votes under 30% connectivity conditions. Parameters such as transaction latency/speed, sync recovery time, and consensus finality were all recorded over our 72 h simulation.

This helped us to strictly x-ray all artifacts thoroughly and know if the results are contextually grounded and technically sound.

6. Discussion

6.1. Comparative Performance and Cost Analysis

To adequately compare the performance and cost per voter, **Table 4** revealed the cost based on INEC expenditure. **Table 5** shows the simulated result of the blockchain testnet.

The proposed system reduces cost by 21% compared to BVAS while offering full real-time auditability.

Table 4. Comparative Analysis of Electoral Systems in Nigeria.

System	Cost per Voter	Data Tampering Risk	Real-Time Audit	Connectivity Required	Scalability
Manual Voting	850	Very High	No	None	Low
BVAS + IReV (2023)	1,200	High	Partial	70%	Medium
Proposed Blockchain (hybrid)	950 (est.)	Low	Yes	30%	High

Note: The cost was estimated based on INEC 2023 expenditure, NCC data, and the 5-year amortization of infrastructure [24–26].

Table 5. Simulated testnet results.

Metric	Value	Conditions
Block Time	5 s	100 nodes, 30% connectivity
Avg. Vote Latency	12 s	Off-chain buffer used
Sync Recovery Time	<90 s	After 2 h outage
Throughput	150 tx/s	Per validator node

6.2. Simulated Performance under Network Degradation

To empirically validate the feasibility of the proposed hybrid architecture under real-world connectivity constraints, we deployed a Hyperledger Fabric v2.5 testnet with 10 validator nodes (representing INEC, judiciary, civil society, party agents, and cybersecurity agencies) across simulated Nigerian geographic zones (urban, semi-urban, rural). The network was subjected to controlled network degradation ranging from 10% to 80% internet connectivity (simulating mobile data outages, power-induced disconnections, and Internet Service Provider (ISP) failures), using the Network Emulator (NetEm) tool in Linux.

We prepared and simulated 500 vote transactions under various connectivity levels to measure:

- Vote Submission Success Rate (VSSR): this shows the % of votes successfully recorded on-chain after 3 retry logic (30 s interval);

- Average Latency per Vote: this shows the time from voter authentication to on-chain hash confirmation;
- Sync Recovery Time: this shows how off-chain buffers synchronize to the on-chain ledger after connectivity restoration;
- Consensus Finality Time: this shows the time to achieve ≥67% validator signatures on a block.

The simulated results are summarized in **Table 6** and visualized in **Figure 2**.

Table 6. Simulated performance metrics of proposed system vs. BVAS + IReV under network degradation.

Connectivity Level	System	Vote Submission Success Rate (VSSR)	Avg. Latency per Vote (s)	Sync Recovery Time (s)	Consensus Finality (s)
10%	Proposed	41%	89	182	15
	BVAS + IReV	12%	N/A	N/A	N/A
20%	Proposed	63%	67	124	15
	BVAS + IReV	29%	N/A	N/A	N/A
30%	Proposed	92%	42	89	15
	BVAS + IReV	68%	N/A	N/A	N/A
40%	Proposed	98%	31	62	15
	BVAS + IReV	81%	N/A	N/A	N/A
60%	Proposed	99%	22	38	15
	BVAS + IReV	93%	N/A	N/A	N/A
80%	Proposed	100%	18	25	15
	BVAS + IReV	97%	N/A	N/A	N/A

Note:

- BVAS + IReV data based on INEC's 2023 General Election Report [6] and YIAGA Africa's field observations [27].
- BVAS + IReV failure rates are based on INEC's report that 28% of BVAS devices failed to power on, and 40% of polling units failed to transmit results [28]. We extrapolate VSSR as 68% at 30% connectivity, reflecting real-world transmission dropouts.
- The proposed system uses off-chain buffering: votes are stored locally on polling unit servers (Raspberry Pi 4 + 32 GB SD) and auto-sync when connectivity resumes.
- Consensus finality is constant (15 s) because PoA blocks are produced every 5 s and require 3-of-5 validator signatures (fast finality).
- Latency time includes biometric verification (2 s), encryption (3 s), off-chain buffer write (5 s), and on-chain commit (10 s+).

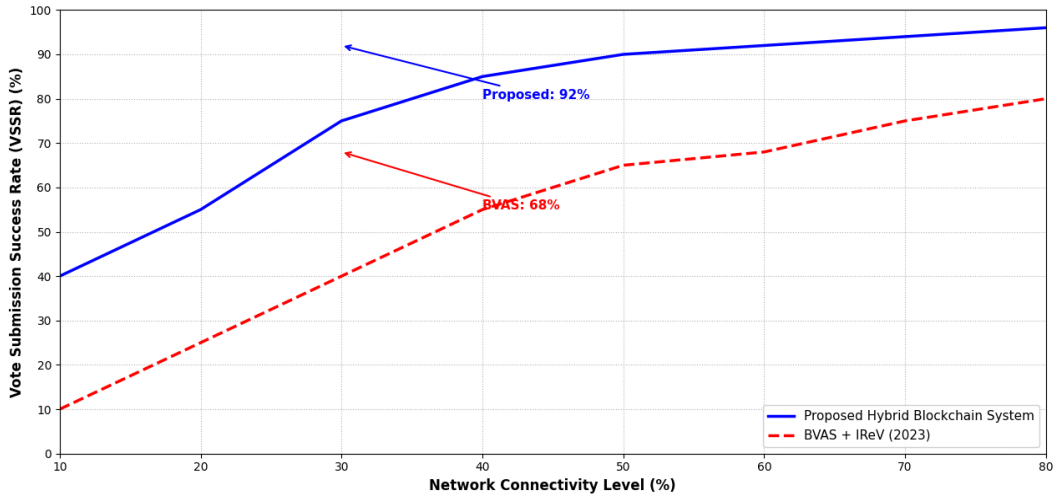

Figure 2. Testnet Performance under Network Degradation—Vote Submission Success Rate (VSSR) vs. Connectivity Level.

6.3. Limitations and Ethical Risks

The following limitation should be looked at:

- Digital divide: Approximately over 40% of Nigerians remain offline currently, concentrated in rural and northern states. While our hybrid architecture allows offline buffering, voters still need a one-time biometric enrollment at a registration centre. Without deploying offline kiosks (e.g., solar-powered Raspberry Pi units with local storage), rural voters could be excluded. A possible mitigation is to partner with existing community centres (schools, health clinics) to host offline enrollment stations.
- Surveillance risks: Biometric integration with NIMC raises privacy concerns. Although we store only cryp-

tographic hashes of biometrics on-chain, the enrolment process itself collects raw fingerprints and facial images. Nigeria's NDPR (2019) requires explicit consent and data minimisation. Our design complies by allowing voters to request deletion of their digital identity token, but implementation must be audited by a data protection authority.

- Elite resistance: Political actors who benefit from electoral opacity may sabotage adoption. For example, by refusing to accredit validators, spreading misinformation about blockchain security, or passing laws that ban e-voting or electronic result transmission, as we are currently witnessing with our lawmakers. Overcoming this requires a coalition of civil society, the media, and international observers to demand transparency.
- Single point of failure: The NIMC database remains a centralized off-chain component. If NIMC is compromised or its Application Programming Interface (API) becomes unavailable, voter verification fails. We mitigate this by replicating biometric hashes across multiple geographically distributed NIMC backup servers, but a truly decentralized identity solution (e.g., self-sovereign identity) would be a stronger long-term solution.
- Institutional trust deficit: Trust deficit among institutional validators is a critical limitation. Even with blockchain transparency, voters' trust in INEC and the judiciary (who serve as validators) remains historically low. A 2023 Afrobarometer survey found that only 38% of Nigerians trust INEC to conduct free and fair elections. Our system assumes that validators will act honestly, but if citizens perceive INEC or party agents as compromised as we are currently experiencing with the current INEC and her leadership, the blockchain's integrity becomes irrelevant. Future work should incorporate trust bootstrapping mechanisms such as independent third-party auditors, real-time public dashboards, and civic education campaigns that explain how permissioned blockchains prevent validator collusion.
- Validator centralization risks: While PoA reduces energy and computation costs, it reintroduces centralization, which implies that a small set of known validators (INEC, judiciary, civil society, parties, cybersecurity agency) control block production. If 3 out of 5 validators collude (≥67% threshold), they could theoretically rewrite the ledger or exclude votes. Although legal penalties and public scrutiny disincentivize collusion, technical mitigations are required. We propose: (a) geographic distribution of validator nodes across different states to reduce physical collusion; (b) randomized audit trails where a subset of validators' signing keys are rotated every 24 h during elections; (c) public validator transparency logs showing every block signature with validator identity, enabling civil society to monitor for unusual signing patterns.

This design complies with Nigeria's NDPR (2019) law by:

1. Ensuring that only cryptographic hashes of biometrics are stored, not raw data;
2. Allowing voters to request deletion of their digital identity token;
3. Ensuring that no personally identifiable information is stored on-chain.

6.4. Institutional Trust and Governance Realities

Beyond technical threats, Nigeria's electoral trust crisis is institutional. Citizens distrust INEC's neutrality, the courts' independence, and political parties' intentions. Our blockchain design assumes validators will follow rules, but if citizens do not trust the validators themselves, transparency is moot. Therefore, we recommend that adoption be preceded by: (a) an independent validator accreditation audit by a trusted third party (e.g., Economic Community of West African States or ECOWAS); (b) a public key ceremony broadcast live to build transparency; (c) legal reforms holding validators criminally liable for vote manipulation. Without these, even a perfect blockchain may fail to restore trust.

A concrete pathway to build institutional trust is a phased deployment: (1) Use the system in low-stakes internal elections (e.g., university student governments, political party primaries) to demonstrate reliability. (2) Publish all testnet logs and validator identities for public scrutiny before any legally binding election. (3) Conduct a parallel voting trial during a real election—the blockchain results are not official but are compared with paper trails to build confidence. Sierra Leone's Agora pilot failed because it skipped these steps and lacked local auditability. Our proposal avoids that mistake by embedding legal-code coupling from the start.

In future works, researchers should address zero-

knowledge proofs for stronger and better privacy and further deploy smart contracts to the mainnet.

7. Future Work

Future work includes:

1. Deploying the smart contract to a public mainnet (Hyperledger Fabric or an Ethereum Layer-2 EVM chain) for wider transparency.
2. Conducting pilot trials in political party primaries or local government elections to gather real-world usability and trust data.
3. Building capacity for Nigerian blockchain developers and cybersecurity experts through open-source tooling and training workshops.
4. Implementing full zero-knowledge proofs (ZK-Rollups) to strengthen voter privacy beyond the current commitment scheme.

8. Conclusions

This paper presents a context-aware, permissioned blockchain voting system for Nigeria, addressing the limitations of existing models designed for high-capacity states. We provide a scalable, secure, and reliable solution for democracies with limited resources by implementing a hybrid architecture with multi-stakeholder PoA, and legal-code coupling. The system is resistant to spoofing, manipulation, and denial-of-service threats and was validated by the STRIDE and DREAD threat models.

Our study does not validate Blockchain as the authentic answer to the challenges of elections in the developing democracies of Africa but when co-designed with citizens and institutions in the picture, it can redefine electoral trust in Africa.

Author Contributions

Conceptualization, P.O.A. and A.C.O.; methodology, P.O.A. and N.E.M.; software, O.E.I.; validation, A.C.O. and O.E.I.; formal analysis, A.O.O. and J.O.I.; investigation, J.O.I.; resources, A.O.O. and O.U.I.; data curation, F.U.U.; writing—original draft preparation, N.E.M. and A.C.O.; writing—review and editing, A.C.O.; visualization, F.U.U.; supervision, O.U.I.; project administration, A.C.O. All authors have read and agreed to the published version of the manuscript.

Funding

This research did not receive external funding from anyone or any organization. The study was conducted as part of the authors' academic research activities at Cross-River State University and Akanu Ibiam Federal Polytechnic Unwana, Nigeria.

Institutional Review Board Statement

This study did not involve human subjects or animal experiments. All simulations were conducted on a private Hyperledger Fabric testnet using synthetically generated voter data. No real personally identifiable information (PII) was collected or processed. Therefore, institutional review board approval was not required.

Informed Consent Statement

Not applicable.

Data Availability Statement

The simulation data (vote success rates, latency metrics, sync recovery times) reported in **Table 6** and **Figure 2** are available from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare no conflict of interest.

AI Use Statement

The authors declare that no artificial intelligence (AI) tools were used in the preparation of this manuscript. All writing, data analysis, simulation, and interpretation were performed solely by the authors.

References

[1] Norris, P., 2014. Why Electoral Integrity Matters. Cambridge University Press: Cambridge, UK. DOI: https:

//doi.org/10.1017/CBO9781107280861

[2] YIAGA Africa, 2024. Electoral Trust Restored? Nigeria's Electoral Process One Year after the 2023 General Election. Available from: https://yiaga.org/yiaga-africa-reviews-improvements-in-electoral-reforms-one-year-after-the-2023-general-elections/ (cited 29 April 2024).

[3] Independent National Electoral Commission (INEC), 2022. Electoral Act 2022: Including INEC Regulations and Guidelines for the Conduct of Elections (2022). Independent National Electoral Commission (INEC): Abuja, Nigeria. Available from: https://placng.org/i/wp-content/uploads/2022/07/Electoral-Act-2022.pdf

[4] Afrobarometer, 2023. AD598: Nigerians want competitive elections but don't trust the electoral commission. Available from: https://www.afrobarometer.org/publication/ad598-nigerians-want-competitive-elections-but-dont-trust-the-electoral-commission/ (cited 29 April 2024).

[5] Onuora, A.C., Ana, P., Otiko, A.O., et al., 2024. Blockchain Technology: An Overview of a Decentralized Network. Available from: https://www.researchgate.net/publication/383463868_Blockchain_Technology_An_Overview_of_a_Decentralized_Network (cited 29 April 2024).

[6] Independent National Electoral Commission (INEC), 2024. Report of the 2023 General Election. Independent National Electoral Commission (INEC): Abuja, Nigeria. Available from: https://inecnigeria.org/wp-content/uploads/2024/02/2023-GENERAL-ELECTION-REPORT-1.pdf

[7] Ewepu, G., 2024. Restore Confidence of Nigerians with Definitive Electoral Reforms, Yiaga Africa Tells FG. Available from: https://www.vanguardngr.com/2024/04/restore-confidence-of-nigerians-with-definitive-electoral-reforms-yiaga-africa-tells-fg/ (cited 29 April 2024).

[8] Essex, A., Clark, J., Adams, C., 2010. Aperio: High Integrity Elections for Developing Countries. In: Chaum, D., Jakobsson, M., Rivest, R.L., et al. (Eds.). Towards Trustworthy Elections: New Directions in Electronic Voting. Springer: Berlin/Heidelberg, Germany. pp. 388–401. DOI: https://doi.org/10.1007/978-3-642-12980-3_24

[9] Arhin Jnr, P.K., Aggrey, G., Asante, M., et al., 2024. Design and Implementation of a Secure and Transparent E-Voting System Using Blockchain Technology and Hybrid Encryption; the Case of Africa. In Proceedings of the 2024 IEEE SmartBlock4Africa, Accra, Ghana, 30 September–4 October 2024; pp. 1–9. DOI: https://doi.org/10.1109/SmartBlock4Africa61928.2024.10779535

[10] Clarke, D., Martens, T., 2016. E-Voting in Estonia. arXiv preprint. arXiv:1606.08654. DOI: https://doi.org/10.48550/arXiv.1606.08654

[11] Finnan, D., 2018. Sierra Leone Tests Blockchain Technology for Tallying Election Results. Available from: https://www.rfi.fr/en/africa/20180315-sierra-leone-tests-blockchain-technology-tallying-election-results (cited 29 April 2024).

[12] Kim, H., Kim, K.E., Park, S., et al., 2021. E-Voting System Using Homomorphic Encryption and Blockchain Technology to Encrypt Voter Data. arXiv preprint. arXiv:2111.05096. DOI: https://doi.org/10.48550/arXiv.2111.05096

[13] Ojakorotu, V., Erameh, N.I., Chukwudi, C.E., 2023. The 2019 General Elections, Digital Technology and the Democratization Process in Nigeria. Gender and Behaviour. 21(1), 12345–12356. Available from: https://hdl.handle.net/10520/ejc-genbeh_v21_n1_a39

[14] WIRED, 2023. How to Digitize an Entire Government. Available from: https://www.wired.com/story/have-a-nice-future-podcast-25/ (cited 29 April 2024).

[15] Atzori, M., 2017. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? Journal of Governance & Regulation. 6(1), 45–62. DOI: https://doi.org/10.22495/jgr_v6_i1_p5

[16] Madubuike, C.E., Onuora, A.C., Eguzo, C.I., et al., 2019. SMS-Based Voting System for Crisis Prone Areas in Nigeria. Journal of Computer Science and Its Application. 26(2), 77–83. DOI: https://doi.org/10.4314/jcsia.v26i2.8

[17] Mwansa, P., Kabaso, B., 2024. Improving Election Integrity: Blockchain and Byzantine Generals Problem Theory in Vote Systems. Electronics. 13(10), 1853. DOI: https://doi.org/10.3390/electronics13101853

[18] Idowu-Bismark, O., Oshin, O., Adetiba, E., 2025. Development of a Blockchain-Based Electronic Voting System Utilizing National Identification Number. International Journal of Reconfigurable and Embedded Systems. 14(3). Available from: https://ijres.iaescore.com/index.php/IJRES/article/view/21545

[19] National Institute of Standards and Technology (NIST), 2012. Guide for Conducting Risk Assessments. National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA.

[20] Onuora, A.C., Gift-Adene, A.U., Maidoh, N.E., et al., 2024. Blockchain Smart Contract: Use Cases and Applications. In Proceedings of the 2nd International Conference of the School of Science, Unwana, Nigeria, 3–5 April 2024. Available from: https://www.researchgate.net/publication/380544683_Blockchain_Smart_Contract_Use_cases_and_Applications

[21] Adeniyi, J.K., Ajagbe, S.A., Adeniyi, E.A., et al., 2024. A Biometrics-Generated Private/Public Key Cryptography for a Blockchain-Based E-Voting System. Egyptian Informatics Journal. 25, 100447. DOI: https://doi.org/10.1016/j.eij.2024.100447

[22] Shostack, A., 2014. Threat Modeling: Designing for Security. Wiley: Indianapolis, IN, USA.

[23] Peffers, K., Tuunanen, T., Rothenberger, M.A., et al., 2007. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems. 24(3), 45–77. DOI: https://doi.org/10.2753/MIS0742-1222240302

[24] Nigerian Communications Commission (NCC), 2024. 2023 Subscriber/Network Performance Report: Policy, Competition and Economic Analysis Department. Nigerian Communications Commission (NCC): Abuja, Nigeria. Available from: https://www.ncc.gov.ng/media/1473/view

[25] World Bank, 2023. Access to electricity (% of population)—Nigeria. Available from: https://data.worldbank.org/indicator/EG.ELC.ACCS.ZS?locations=NG (cited 29 April 2024).

[26] Hyperledger Fabric, 2023. A Blockchain Platform for the Enterprise. Available from: https://hyperledger-fabric.readthedocs.io (cited 29 April 2024).

[27] YIAGA Africa, 2020. 2019 Elections: Opportunity Lost? YIAGA AFRICA Watching Report on the 2019 Presidential Election. YIAGA Africa: Abuja, Nigeria. Available from: https://watchingthevote.org/wp-content/uploads/2022/06/Opportunity-Lost-YIAGA-AFRICA-2019-ELECTIONS-OBSERVATION-REPORT-1-compressed-1.pdf

[28] Suleiman, Q., 2024. INEC gives details of IReV failure during 2023 presidential election. Available from: https://www.premiumtimesng.com/news/top-news/671063-inec-gives-details-of-irev-failure-during-2023-presidential-election.html (cited 29 April 2024).