Blockchain-Based Secure and Transparent Electoral Systems: A Technical Framework for Developing Democracies

Ogbunude Festus Okechukwu[1]; Onuora Augustine Chidiebere[2];
Ekuma Daberechi David[3]; Madubuike Chibuike Ezeocha[4];
Okeoma Chinwendu Amarachi[5]

[1,5]Department of Computer Science, Federal Polytechnic,
Ngodo Isuochi, Abia State, Nigeria
[2,4] Department of Computer Science, Akanu Ibiam Federal
Polytechnics Unwana, Ebonyi State. Nigeria
[3] Department of Computer Science, Ihechukwu Madubuike
Institute of Technology, Abia State, Nigeria

Abstract
Persistent electoral irregularities—ranging from vote manipulation and ballot stuffing to logistical failures and post-election violence—continue to undermine democratic consolidation across developing democracies. Nigeria, Africa's largest democracy, epitomizes this crisis, where recurrent allegations of fraud, digital failures, and institutional mistrust have eroded public confidence in electoral outcomes. This paper proposes a secure, transparent, and technically robust blockchain-based electoral framework tailored for developing democracies. Leveraging the core attributes of blockchain—immutability, decentralization, real-time auditability, and cryptographic security—we design a technical architecture for voter registration, ballot casting, vote tallying, and public verification. The system integrates smart contracts, Proof of Authority (PoA) consensus, cryptographic identity verification, and zero-knowledge proofs to ensure integrity, privacy, and resilience. We analyze implementation challenges including the digital divide, cybersecurity threats, and legal gaps, and propose a phased, stakeholder-driven roadmap anchored in Nigeria's institutional context. Comparative insights from Estonia, Sierra Leone, and Brazil underscore the importance of local ownership, institutional autonomy, and civic literacy. The paper contributes a practical, context-sensitive blueprint for blockchain-based electoral reform, bridging the gap between theoretical innovation and real-world deployment in fragile democratic ecosystems.

Keywords: Blockchain, Electoral Integrity, Digital Democracy, Smart Contracts, Voter Trust, Decentralization, E-Voting

1. Introduction

1.1.Contextual Background: Electoral Crises in Developing Democracies

In many developing democracies, elections have become ritualistic exercises—frequently held but rarely trusted. Despite formal democratic transitions, the integrity of electoral processes remains compromised by systemic flaws such as vote-buying, ballot stuffing, result tampering, and the politicization of electoral institutions [1], [2]. These irregularities fuel public distrust, political polarization, and civic apathy, weakening the very accountability mechanisms that elections are meant to reinforce.

Sub-Saharan Africa presents a paradox of "electoral ritualism"—where democratic form exists without substantive legitimacy [3]. Nigeria, Kenya, Uganda, and Zimbabwe have all experienced elections whose outcomes were contested not only by losing candidates but also by civil society and international observers. In Nigeria, over 60% of citizens lack confidence in the electoral process,

DOI: https://doi.org/10.5281/zenodo.17824707

according to a 2023 Afrobarometer survey [4]. This crisis is not merely procedural; it is existential for democratic legitimacy.

1.2 Nigeria's Electoral Landscape: A Case of Chronic Mistrust

Since the return to civilian rule in 1999, Nigeria has conducted seven general elections. While reforms such as biometric voter registration, Permanent Voter Cards (PVCs), Smart Card Readers, and the INEC Results Viewing (IReV) Portal have been introduced, implementation gaps persist. The 2023 general elections, despite being hailed as technologically advanced, were marred by:

- Widespread BVAS (Bimodal Voter Accreditation System) failures [5]
- Delayed or missing uploads to the IReV portal
- Accusations of digital sabotage and selective result transmission
- Alleged manipulation of collation processes

These failures eroded public trust and reignited debates about the credibility of digital electoral systems.

1.3.BlockchainasaDisruptive Innovation for Electoral Reform

Blockchaintechnology,originallydeveloped for cryptocurrencies, has evolved into a trustless, decentralized ledger system capable of ensuring tamper-proof record-keeping, transparent auditing, and automated enforcement via smart contracts [6]. When applied to elections, blockchain can:

- Prevent vote alteration through cryptographic immutability
- Enable real-time auditing by citizens, observers, and political parties
- Reduce human interference in vote counting and collation
- Enhance accessibility for Diaspora and remote voters

In Nigeria, where institutional trust is chronically low, blockchain offers a technologically anchored solution to restore credibility and accountability [7].

2. Blockchain Architecture for Secure and Transparent Elections

2.1 Consensus Mechanism: Why Proof of Authority (PoA)?

Blockchain relies on consensus mechanisms to validate transactions. Common models include:

Table I: Comparison of Blockchain Consensus

Mechanism	Pros	Cons	Suitability for Elections
Proof of Work (PoW)	**High security, decentralized**	**Energy-intensive, slow**	**Unsuitable**
Proof of Stake (PoS)	**Energy-efficient, faster**	**Risk of wealth-based centralization**	**Limited**
Delegated PoS (DPoS)	**Fast, scalable**	**Oligarchic tendencies**	**Risky**
Proof of Authority (PoA)	**Fast, energy-efficient, accountable**	**Permissioned, requires trusted validators**	**Ideal**

For national elections in developing democracies, Proof of Authority (PoA) is optimal. PoA uses a permissioned network of pre-verified validators—such as INEC officials, judiciary representatives, civil society observers, and cybersecurity experts—who are accountable for validating votes [8].

Advantages of PoA for Nigeria:

- High throughput: Can handle millions of transactions (votes) per hour.
- Low latency: Enables real-time result transmission.
- Governance alignment: Validators are legally and institutionally accountable.
- Energy efficiency: Critical for regions with unstable power supply.

DOI: https://doi.org/10.5281/zenodo.17824707

Table II: Comparison of Consensus Mechanisms for Electoral Applications

Feature	PoW	PoS	DPoS	PoA
Decentralization	High	Medium	Low	Low
Speed	Low	Medium	High	High
Energy Use	Very High	Medium	Low	Very Low
Accountability	None	Limited	Limited	High
Suitability for Elections	No	No	No	Yes

1. Decentralization

Proof of Work (PoW) offers the highest level of decentralization, as any node can participate in mining (e.g., Bitcoin). However, this leads to mining centralization due to hardware and energy costs, undermining true decentralization in practice.

Proof of Stake (PoS) and Delegated PoS (DPoS) reduce decentralization by concentrating validation power among stakeholders or elected delegates, increasing risks of oligarchic control.

Proof of Authority (PoA) is inherently permissioned and centralized, but this is advantageous in electoral contexts where validators must be accountable public officials (e.g., INEC officers, judiciary reps).

2. Speed (Transaction Throughput and Latency)

PoW is slow (e.g., Bitcoin: ~7 TPS, 10-minute block time), making it unsuitable for real-time vote collation.

PoS improves speed (~30–100 TPS), but still lags behind national election demands.

DPoS and PoA achieve thousands of transactions per second (TPS) with sub-second finality—critical for processing millions of votes within hours.

3. Energy Use

PoW is energy-intensive (Bitcoin consumes ~150 TWh/year), unsustainable for a developing nation like Nigeria with unstable power infrastructure.

PoS, DPoS, and PoA are energy-efficient, with PoA being the most sustainable due to minimal computational overhead.

4. Accountability

PoW, PoS, DPoS: Validators are anonymous or pseudonymous, making it impossible to hold them accountable for malicious behavior.

PoA: Validators are pre-approved, known entities (e.g., INEC, NIMC, CSOs), whose identities and actions are publicly logged. This enables legal and institutional accountability, essential for electoral integrity.

5. Suitability for Elections

PoW, PoS, DPoS are designed for open, permissionless networks—ideal for cryptocurrencies but risky for sovereign elections due to lack of oversight.

PoA is ideal because it:

- Supports regulated participation
- Ensures fast, auditable, and energy-efficient consensus
- Aligns with national legal frameworks
- Enables real-time transparency without sacrificing security

For Nigeria's electoral system, PoA is the only viable consensus mechanism due to its balance of speed, accountability, and institutional compatibility.

2.2 Smart Contracts: Automating Electoral Integrity

Smart contracts are self-executing code embedded in the blockchain that enforce rules without human intervention [9]. In elections, they can:

- Validate voter eligibility using NIMC-linked identities
- Prevent double voting by locking out duplicate entries
- Trigger automated tallying at a predefined time
- Enforce legal rules (e.g., disqualification of delayed results per Electoral Act 2022)

Example Smart Contract Logic (python Pseudocode):

```
def cast_vote(voter_id, encrypted_ballot):
if voter_id in registered_voters and not voted[voter_id]:
blockchain.append(encrypted_ballot)
voted[voter_id] = True
emit_vote_cast_event(voter_id)
else:
revert("Invalid or duplicate vote")
```


DOI: https://doi.org/10.5281/zenodo.17824707

This automated enforcement reduces opportunities for manipulation and ensures procedural compliance.

A solidity smart contract snippet

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract SecureElection {
// Voter structure
struct Voter {
bool registered;
bool voted;
uint256 vote;
}
// Candidate mapping (candidate ID => vote count)
mapping(uint256 => uint256) public votesReceived;

// Voter registry (NIN hash => Voter)
mapping(bytes32 => Voter) public voters;
// Election parameters
uint256 public candidateCount;
uint256 public electionEndTime;
address public electionAuthority;
bool public electionActive;
// Events
event VoteCast(bytes32 indexed voterHash, uint256 candidateId);
event ElectionEnded(uint256 timestamp);
// Modifier: Only authorized entity can call
modifier onlyAuthority() {
require(msg.sender == electionAuthority, "Not authorized");
_;
}
// Constructor
constructor(uint256 _candidateCount, uint256 _durationHours) {
candidateCount = _candidateCount;
electionAuthority = msg.sender;
electionEndTime = block.timestamp + (_durationHours * 1 hours);
electionActive = true;
}
// Register voter (called by INEC/NIMC backend)
function registerVoter(bytes32 _voterHash) external onlyAuthority {
require(!voters[_voterHash].registered, "Voter already registered");
voters[_voterHash] = Voter(true, false, 0);
}
// Cast vote
function vote(bytes32 _voterHash, uint256 _candidateId) external {
require(electionActive, "Election not active");
require(block.timestamp < electionEndTime, "Election ended");
require(_candidateId > 0 && _candidateId <= candidateCount, "Invalid candidate");
require(voters[_voterHash].registered, "Voter not registered");
require(!voters[_voterHash].voted, "Voter already voted");
voters[_voterHash].voted = true;
voters[_voterHash].vote = _candidateId;
votesReceived[_candidateId]++;

emit VoteCast(_voterHash, _candidateId);
}
// End election (automated or manual)
functionendElection()external onlyAuthority {
require(block.timestamp>= electionEndTime, "Election not over");
electionActive = false;
emit ElectionEnded(block.timestamp);
}
// Get total votes for candidate
functiontotalVotesFor(uint256 _candidateId)externalviewreturns (uint256) {
return votesReceived[_candidateId];
}
// Check if voter has voted
function hasVoted(bytes32 _voterHash) external view returns (bool) {
return voters[_voterHash].voted;
}
}
```

Key Features:

- Uses hashed NIN (National Identity Number) for privacy
- Prevents double voting
- Enables real-time auditing via events
- Supports automated tallying
- Can be integrated with BVAS/NIMC backend

2.3 Cryptographic Identity Verification: Securing the Ballot Box

To prevent impersonation, ghost voting, and duplicate registration, the system integrates biometric authentication with blockchain-based digital identity, creating a secure, singular, and tamper-proof voter registry.
Workflow in Detail

DOI: https://doi.org/10.5281/zenodo.17824707

Voter Registration with NIMC

- Every eligible voter registers with the National Identity Management Commission (NIMC).
- Biometric data (fingerprint, facial scan) and demographic details are collected and verified.
- A National Identification Number (NIN) is issued.
- Cryptographic Hashing and Blockchain Storage
- The NIN and biometric hash (not raw data) are stored on the blockchain.
- Example: keccak256(NIN + fingerprint_hash) → 0xabc123...
- This hash serves as the unique digital identity on-chain, ensuring immutability and non-repudiation.

Authentication during Voting

- At the polling unit, the voter uses a BVAS-like device to authenticate via fingerprint or facial recognition.
- The system verifies the biometric match against NIMC's database (off-chain).
- If valid, a one-time encrypted token (e.g., JWT) is issued, allowing access to the digital ballot.

Ballot Casting and Anonymity

- The voter selects a candidate via a mobile or kiosk interface.
- The vote is encrypted and recorded on the blockchain with the token, not the identity.
- The link between voter and vote is broken, preserving ballot secrecy.

This ensures:

- Singular registration (no duplicates)
- Anonymity (vote not linked to identity)
- Tamper-proof audit trail

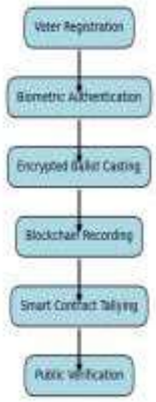

Figure 1: Blockchain Voting Flowchart

3. Security and Transparency: A Dual Imperative

3.1.Threat Modeling and Mitigation Strategies

While blockchain is secure at the protocol level, surrounding systems are vulnerable.

Table III: Threat Modeling and Mitigation in Blockchain Voting

Threat	Risk Level	Mitigation Strategy
SybilAttack (fake identities)	**High**	**Biometric binding to NIMC, validators verification**
Coercion/Re-voting	**Medium**	**Allow multiple votes; only last vote counts**
DDoS Attacks	**High**	**Redundant nodes, cloud-based load balancing**
Phishing/Social Engineering	**High**	**Voter education, multi-factor authentication**

DOI: https://doi.org/10.5281/zenodo.17824707

Threat	Risk Level	Mitigation Strategy
Quantum Computing	Future Risk	Design with post-quantum cryptography (e.g., lattice-based)

3.2 Privacy vs. Transparency: The Core Tension

A major challenge is balancing transparency (public auditability) with privacy (secret ballot).
Proposed Solution:

- Votes are encrypted before being recorded on-chain.
- Zero-Knowledge Proofs (ZKPs) allow verification of vote validity without revealing content.
- Homomorphic Encryption enables tallying without decryption [10].
- Voters receive verifiable receipts (not their vote) to confirm inclusion in the ledger.

TableIV:Privacy-Preserving Techniques in Blockchain Voting

Technique	Function	Implementation Complexity
Zero-Knowledge Proofs (ZKPs)	Prove vote validity without revealing choice	High
Homomorphic Encryption	Tally encrypted votes	Very High
Mixnets	Shuffle votes to Anonymize	Medium
Receipt-Free Voting	Prevent coercion via fake receipts	Medium

For initial deployment, a hybrid model using encrypted votes + verifiable receipts is recommended.

4. Technical Challenges and Interoperability

4.1 Integration with Existing Systems

Nigeria already uses:

- BVAS for biometric accreditation
- IReV Portal for result transmission

Integration Strategy:

- Phase 1: Use blockchain for result collation only (votes transmitted via IReV → recorded on blockchain)
- Phase 2: Replace BVAS with blockchain-authenticated login
- Phase 3: Full end-to-end blockchain voting

4.2 Scalability and Performance

- Hyperledger Fabric or Ethereum (PoA) can support 10,000+ TPS [12].
- Sharding and layer-2 solutions can further enhance scalability.
- Load testing and adversarial simulations are essential before national deployment.

5. Comparative Insights from Global Pilot Programs

TableV:GlobalBlockchainVoting Experiments

Country	Year	Scope	Outcome	Lessons for Nigeria
Estonia	2005–present	i-Voting with blockchain audit	High trust, 44% online voting	Strong digital ID is key

DOI: https://doi.org/10.5281/zenodo.17824707

Country	Year	Scope	Outcome	Lessons for Nigeria
Sierra Leone	2018	Results collation only	Fast, transparent	Avoid foreign platform control
West Virginia, USA	2018–2020	Military absentee voting	Increased access	Cybersecurity concerns
Switzerland	2018–2022	Cantonal trials	Suspended due to flaws	Rigorous auditing needed
India	Ongoing	EVMs, no blockchain	High reliability	Incremental tech adoption

A number of countries and jurisdictions have piloted blockchain technologies for elections. These examples provide insight into the feasibility, challenges, and outcomes of early adoption.

- **Estonia**
  Although Estonia's digital voting system (i-Voting) is not purely blockchain-based, it incorporates blockchain for securing the integrity of vote records and audit trails. Estonia's success demonstrates the value of integrated digital infrastructure, legal support, and public trust in technology.

- **Sierra Leone (2018)**
  In a pilot program during its presidential elections, the National Electoral Commission partnered with Agora Technologies to use blockchain to record, verify, and tally votes in one district. While not adopted nationwide, the pilot showed potential for transparency and speed—though questions of sovereignty and external involvement were raised.

- **West Virginia, USA**
  Used blockchain-based mobile voting for overseas military personnel between 2018 and 2020. Though results were promising in increasing accessibility, concerns emerged around cybersecurity vulnerabilities, leading to a pause in further expansion.

- **Switzerland:**
  Conducted several pilot blockchain e-voting trials at the cantonal level. The trials were halted following an independent cryptographic audit that revealed vulnerabilities—highlighting the importance of rigorous testing before deployment.

- **Russia and India:**
  Both countries have explored blockchain-based voting, especially for party primaries and local elections.
  What we can deduce from the above countries include;

- Local ownership is critical [13].
- Institutional trust must precede technological adoption [14].
- Phased implementation reduces risk [15].

6. Implementation Roadmap for Nigeria (2025–2030)

Implementing blockchain voting in Nigeria requires a phased, inclusive, and context sensitive approach. Given the political, infrastructural, and legal complexities of the Nigerian environment, a successful rollout must be gradual—starting from pilot programs to national-level scale-up, backed by enabling laws, strategic partnerships, and mass voter education.

Phase 1: Legal and Institutional Foundation (0–12 Months)

Key Activities

- Amend Electoral Act 2022 to provide legal backing for blockchain voting systems.
- Establish a multi-stakeholder Electoral Technology Reform Task Force led by INEC, including the National Assembly, ICT experts, CSOs, and the private sector.
- Conduct a national regulatory sandbox to test blockchain applications under controlled legal conditions (similar to Nigeria's fintech model under the Central Bank).
- Draft technical standards and security protocols in collaboration with cybersecurity agencies and international partners.

Expected Outcomes

- Legal clarity for experimentation and pilot testing
- INEC alignment with innovation strategy

DOI: https://doi.org/10.5281/zenodo.17824707

- Institutional commitment to long-term reform

Phase 2: Infrastructure Development and Pilot Testing (12–24 Months)

Key Activities

Develop a secure blockchain voting platform in partnership with Nigerian software developers and blockchain companies.

Launch pilot tests in:

- Political party primaries
- Diaspora voting (remote, digital voting)
- Local council elections in selected states

Integrate the platform with NIMC digital ID system for voter authentication.

Establish a national blockchain electoral observatory to audit, document, and report on performance.

Expected Outcomes

- Proof-of-concept demonstrations in live environments
- Identification of scalability and user-experience challenges
- Data-driven basis for future investment and adoption

Phase 3: Voter Education and Stakeholder Sensitization (Concurrent)

Key Activities

- Launch a multi-channel civic education campaign to raise public awareness and build trust in blockchain voting.
- Use radio, TV, social media, religious institutions, and community leaders to demystify the process.
- Create training modules for electoral officers, political party agents, and election observers.

Expected Outcomes

- Increased digital literacy and reduced skepticism
- Wider civic participation in reform processes
- Reduced vulnerability to misinformation

Phase 4: Gradual Scale-Up and Electoral Integration (24–48 Months)

Key Activities

- Expand blockchain voting to state assembly and gubernatorial elections in digitally prepared states.
- Strengthen cybersecurity infrastructure and update INEC's digital systems for interoperability.
- Develop real-time analytics dashboards for election monitoring and result verification.
- Introduce smart contracts for automatic vote tallying and results announcement in pilot areas.

Expected Outcomes

- Scalable technical infrastructure
- Strengthened institutional capacity
- Transition from pilots to mainstream adoption

Phase 5: Full National Deployment (48–72 Months)

Key Activities

- Implement blockchain voting nationally during general elections, starting with presidential and National Assembly races.
- Institutionalize blockchain voting within INEC's standard procedures.
- Conduct post-election audits to refine system weaknesses.

Expected Outcomes

- End-to-end transparent elections with immutable records
- Significantly reduced allegations of fraud and result manipulation
- Public restoration of confidence in the electoral process

Implementation Principles

To ensure success, the strategy must be governed by five core principles:

1. Inclusiveness: No group should be digitally excluded
2. Legal Soundness: All implementations must be backed by law
3. Security: Systems must be robust against cyberattacks
4. Transparency: Open reporting, auditing, and public monitoring
5. Phased Flexibility: Learn from each phase to improve the next

DOI: https://doi.org/10.5281/zenodo.17824707

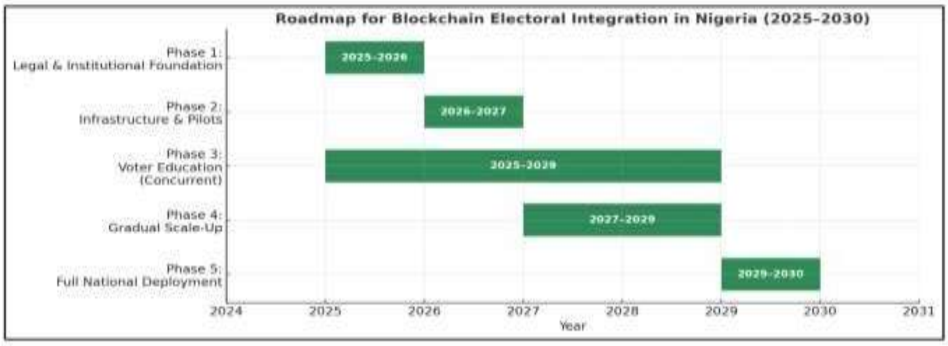

Figure 2: Gantt Chart – Blockchain Electoral Integration Roadmap

Table VI: Global Blockchain Voting Experiments

Phase	Duration	Key Activities	Expected Outcomes
1.Legal& Institutional	**0–12 mo**	**Amend Electoral Act, form task force, regulatory sandbox**	**Legal clarity, stakeholder buy-in**
2. Infrastructure & Pilots	**12–24 mo**	**Build platform, test in primaries, diaspora voting**	**Proof of concept**
3. Voter Education	**Ongoing**	**Civic campaigns, training, media engagement**	**Increased trust, reduced skepticism**
4. Scale-Up	**24–48 mo**	**State elections, smart contracts, real-time dashboards**	**Institutional capacity**
5. National Deployment	**48–72 mo**	**General elections, full blockchain voting**	**Transparent, auditable elections**

Implementation Principles:

- Inclusiveness:Nodigital disenfranchisement
- Legal Soundness: Backed by law
- Security: Resilient to attacks
- Transparency: Open auditing
- Phased Flexibility: Learn and adapt

7. Policy Recommendations

7.1 Legislative Reforms

- Amend Electoral Act 2022 to recognize blockchain ballots [5].
- Establish regulatory sandbox for electoral tech testing.
- Define data protection standards with NDPC.

7.2 Institutional Capacity

- Create INEC Electoral Innovation Unit.
- Train blockchain specialists across departments.
- Strengthen INEC autonomy and funding.

7.3 Infrastructure Development

- Expand internet and power access in rural areas.
- Develop national blockchain standards.
- Support local tech development in universities.

7.4 Public Engagement

- Launch multi-channel civic education.
- Empower CSOs as intermediaries.
- Enable citizen audits via public blockchain explorers.

8. Conclusion and Future Work

Blockchain is not a silver bullet, but a powerful tool for restoring electoral integrity in Nigeria. By combining technical security with institutional transparency, it can shift the narrative from manipulation to accountability.

Future Work:

- Testnet deployment using Hyperledger Fabric.
- Pilot programs in party primaries and local councils.
- Capacity building for Nigerian developers.

The promise of blockchain lies not in its novelty, but in its ability to restore agency and

DOI: https://doi.org/10.5281/zenodo.17824707

trust to citizens. For Nigeria, the path forward is not just technological—but institutional, legal, and civic.

9. References

[1] P. Norris, Democratic Deficit: Critical Citizens Revisited. Cambridge University Press, 2014.

[2] C. Van Ham and S. I. Lindberg, "The myth of the democratic transition? Electoral authoritarianism and regime durability in Africa," Democratization, vol. 22, no. 2, pp. 1–22, 2015.

[3] N. Cheeseman, "Democracy in Africa: Successes, failures, and the struggle for political reform," Cambridge University Press, 2015.

[4] Afrobarometer, "Nigeria: Public confidence in electoral process, 2023," 2023. [Online]. Available: https://afrobarometer.org

[5] INEC, Report on the 2023 General Elections. Independent National Electoral Commission, 2023.

[6] D. Tapscott and A. Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. Penguin, 2016.

[7] F. E. Ikuero et al., "Is e-voting systems based on blockchain technology efficient in Nigeria general elections?" EAI Endorsed Transactions on Security and Safety, vol. 7, no. 25, p. e1, 2021.

[8] A. C. Onuora et al., "Blockchain Technology: An Overview of a Decentralized Network," 2nd International Conference of the School of Science, Akanu Ibiam Federal Polytechnic, 2024.

[9] A. C. Onuora et al., "Blockchain Smart Contract: Use cases and Applications," 2nd International Conference of the School of Science, Akanu Ibiam Federal Polytechnic, 2023.

[10] H. Kim et al., "E-voting system using homomorphic encryption and blockchain technology to encrypt voter data," arXiv, 2021. [Online]. Available: https://doi.org/10.48550/arXiv.2103.12345

[11] NCC, Nigeria Internet Penetration Report Q4 2023. Nigerian Communications Commission, 2023.

[12] S. Chouhan and G. Sharma, "A new era of elections: Leveraging blockchain for fair and transparent voting," arXiv, 2025. [Online]. Available: https://doi.org/10.48550/arXiv.2502.16127

[13] D. Finnan, "Sierra Leone tests blockchain technology for tallying election results," RFI, 2018.

[14] D. Clarke and T. Martens, "E-voting in Estonia," arXiv, 2016. [Online]. Available: https://doi.org/10.48550/arXiv.1606.08654

[15] G. Ohiohka and F. I. Ohiohka, "The imperative of blockchain technology in Nigeria general elections," Int. J. Social Sci. Res. Anthropol., vol. 3, no. 6, 2024.

DOI: https://doi.org/10.5281/zenodo.17824707