Blockchain-Based Electoral Systems as a Remedy for Electoral Fraud: Evidence from Nigeria's Democratic Experience

Anthony C.N. Igwebuike

Center for Information and Communication Engineering Technology University of Port Harcourt

DOI: https://doi.org/10.47772/IJRISS.2026.1013COM0020

Received: 03 May 2026; Accepted: 08 May 2026; Published: 29 May 2026

ABSTRACT

Electoral integrity remains one of the most critical challenges confronting emerging democracies, particularly in sub-Saharan Africa. This article examines the viability of Hyperledger Fabric blockchain technology as a systemic solution to the pervasive electoral fraud, institutional distrust, and process opacity that have undermined democratic governance in Nigeria. Drawing on primary survey data collected from 800 Nigerian voters across all 36 states and the Federal Capital Territory, this study analyses public perceptions of the Independent National Electoral Commission (INEC), identifies the structural weaknesses in Nigeria's electoral framework, and evaluates the technical architecture of a proposed blockchain-based voting system. Survey results reveal that approximately 65% of respondents attribute electoral failures primarily to INEC, while over 85% expressed no confidence in the commission's ability to conduct transparent elections. Respondents overwhelmingly called for tamper-proof, technology-driven electoral systems. The proposed Hyperledger Fabric-based system, incorporating biometric authentication, decentralised ledger technology, and real-time result transmission, is posited as a cost-effective and structurally sound alternative to existing electoral infrastructure. At an estimated implementation cost of approximately 100 billion Naira a fraction of the 400+ billion Naira spent in the 2023 general elections the system offers significant fiscal and democratic value. The article concludes with policy recommendations for institutional reform, regulatory alignment, and phased technological adoption.

Keywords: Blockchain technology, electoral integrity, Hyperledger Fabric, Nigeria, INEC, democratic governance, biometric authentication

INTRODUCTION

Democratic governance is premised on the foundational principle that political power derives from the free and informed consent of the governed. This principle, however, can only be meaningfully operationalized when electoral systems are credible, transparent, and resistant to manipulation. Across the democratic world, the mechanisms through which citizens exercise their franchise have evolved substantially from open ballot systems to secret paper ballots, and more recently to various forms of electronic and biometric-assisted voting. Despite these advances, electoral fraud remains endemic in many emerging democracies, including Nigeria.

Nigeria, Africa's most populous nation with an estimated population of 220 million and approximately 93 million registered voters, has experienced recurring controversies surrounding its electoral processes. The 2023 general elections, in particular, drew widespread condemnation from civil society organisations, international observers, and the aggrieved political class alike. The Independent National Electoral Commission (INEC), which serves as the constitutional body responsible for organising and conducting elections in Nigeria, faced severe criticism for alleged result manipulation, systemic technological failures, voter suppression, and a general lack of transparency in result collation and transmission. The European Union Election Observation Mission (2023) noted significant failures in the transparency and inclusivity of the process, raising fundamental questions about whether the declared results reflected the actual wishes of Nigerian voters.

It is within this context that Igwebuike (2023) proposed the adoption and implementation of Hyperledger Fabric blockchain technology as a comprehensive electoral reform solution. The research, grounded in an extensive nationwide survey and a technical implementation exercise, argues that blockchain's inherent attributes

immutability, decentralisation, transparency, and security make it uniquely suited to addressing the structural deficiencies of Nigeria's electoral architecture. This article synthesises the findings of that research to construct a broader academic argument about the role of distributed ledger technologies in democratic governance, with particular reference to the Nigerian context.

The article proceeds as follows: Section 2 articulates the problem statement; Section 3 presents the research questions; Section 4 reviews relevant theoretical and empirical literature; Section 5 describes the methodology; Section 6 presents the source data and findings; Section 7 discusses the implications of those findings; Section 8 offers policy recommendations; and Section 9 concludes.

Statement of the Problem

The credibility of Nigeria's electoral system has been chronically undermined by a combination of institutional deficiency, technological inadequacy, political interference, and systemic corruption. The 2023 presidential election illustrated these challenges in stark relief. INEC deployed the Bimodal Voter Accreditation System (BVAS) and the INEC Result Viewing Portal (IREV) as technological interventions designed to enhance transparency and prevent result manipulation. However, both systems reportedly experienced significant failures, with INEC officials citing "technical glitches" to explain discrepancies between field-level results and officially announced outcomes explanations that failed to satisfy observers or the electorate.

The fundamental structural problem is the centralisation of result collation. When results from 176,974 polling units across Nigeria are funnelled through a single or limited number of collation centres, the system creates discrete vulnerability points at which data can be intercepted, altered, or suppressed by individuals with access, authority, or political motivation. This architecture, by design or neglect, concentrates enormous electoral power in the hands of a small number of officials who are themselves susceptible to political pressure, bribery, or ideological bias.

Furthermore, the reliance on paper ballots, physical transportation of electoral materials, and manual collation processes in a country of Nigeria's geographic and demographic scale introduces additional layers of logistical risk and human error. The persistent failure to resolve these structural issues after successive election cycles suggests that incremental reforms within the existing paradigm are insufficient. A fundamentally new technological architecture is required one that eliminates human discretion from the most critical stages of the electoral process and replaces it with cryptographically secured, distributed, and auditable records.

Research Questions

This article is guided by the following two research questions:

1. To what extent do Nigerian voters perceive the Independent National Electoral Commission (INEC) as capable of conducting credible, transparent, fraud-resistant elections, and institutional factors underpin this perception?

2. In what ways does Hyperledger Fabric blockchain technology address the structural vulnerabilities of Nigeria's existing electoral infrastructure, and the technical, financial policy preconditions for its effective implementation?

LITERATURE REVIEW

Electoral Integrity and Democratic Governance

Electoral integrity is broadly understood as the extent to which elections conform to international norms and standards throughout the electoral cycle (Norris, 2014). Scholars have identified multiple dimensions of electoral integrity, including the legal framework, voter registration, campaign environment, voting procedures, vote counting, and result verification. In sub-Saharan Africa, structural deficits in several of these dimensions have persistently compromised democratic outcomes. Bratton (2008) and Cheeseman and Klaas (2018) document

how electoral manipulation in African contexts is frequently orchestrated through institutional channels, with electoral management bodies serving as instruments of incumbent advantage rather than neutral arbiters.

In Nigeria, Adejumobi (2007) argues that the gray pattern of election and electioneering is deeply embedded in the country's political culture and is perpetuated by a combination of weak institutions, winner-takes-all political incentives, and a culture of impunity. Agbu (2016) further contends that INEC's lack of genuine institutional independence exemplified by the president's power to appoint its chairman structurally compromises its neutrality and public credibility. These analyses suggest that electoral reform in Nigeria must address both the technical and institutional dimensions of the problem simultaneously.

Blockchain Technology and Electoral Systems

Blockchain technology, first conceptualized by the pseudonymous Satoshi Nakamoto (2008) as the underlying infrastructure for Bitcoin, is a distributed ledger technology in which transactions are recorded in cryptographically linked blocks across a peer-to-peer network. Key properties of blockchain include immutability (records cannot be retroactively altered without network consensus), transparency (all participants can verify the ledger), decentralization (no single point of failure or control), and non-repudiation (all transactions are traceable and attributable).

The application of these properties to electoral systems has attracted growing scholarly and policy interest. Desouza and Somvanshi (2018) examined the pilot use of blockchain in the 2018 West Virginia primary elections and identified its potential to enhance transparency and capture overseas votes securely.

Castillo (2020) documented the use of Ethereum's Etherscan by the Associated Press to monitor the 2020 US presidential election results in real time, demonstrating the technology's capacity for public auditability. Vinnakota (2021) catalogued global instances of blockchain voting, including applications in Sierra Leone, Russia, Japan, and several US states, concluding that the technology was gaining traction as a credible electoral tool.

However, the literature also identifies significant limitations. Jefferson and Verified Voting (2023) argue that blockchain voting systems remain vulnerable to cyber-attacks, particularly at the interface between the voter's device and the blockchain ledger, before ballots are immutably recorded. Specter et al. (2020), in their security analysis of the Voatz platform, identified multiple attack vectors including passive network surveillance, active network interference, and compromised device security that could undermine the integrity and secrecy of blockchain-based voting. These critiques are particularly salient for remote voting applications and underscore the importance of controlled, supervised voting environments for any near-term blockchain electoral deployment.

Hyperledger Fabric as an Electoral Platform

Hyperledger, an umbrella project of open-source blockchain frameworks initiated by the Linux Foundation in 2015 with contributions from IBM, Intel, SAP, and subsequently a broad consortium of technology companies including Samsung, Microsoft, and American Express, provides a permissioned blockchain architecture suited to institutional applications (Hyperledger, 2023). Unlike public blockchains such as Bitcoin or Ethereum, Hyperledger Fabric operates on a permissioned basis, meaning that network participants are known, authenticated, and granted access according to defined roles. This architecture is well-suited to electoral applications, where participant identity and access control are of paramount importance.

Hyperledger Fabric's modularity including configurable consensus mechanisms, support for smart contracts (chaincode) written in Go, Java, or Node.js, and integration with enterprise data systems provides the flexibility necessary to adapt the platform to diverse electoral contexts. Igwebuike (2023) identified Hyperledger Fabric as the preferred blockchain framework for Nigerian electoral reform on the basis of its permissioned architecture, programming flexibility, and the availability of SDKs for integration with biometric hardware platforms.

THEORETICAL FRAMEWORK

This article draws on two complementary theoretical frameworks. First, New Institutionalism (March & Olsen, 1984) provides a lens for understanding how institutional rules, norms, and structures shape and are shaped by electoral behaviour and outcomes. From this perspective, electoral fraud in Nigeria is not merely a matter of individual misconduct but reflects the institutionalization of practices and incentive structures that systematically reward manipulation and penalize compliance. Reform, accordingly, must operate at the institutional level, redesigning the rules and incentives that govern electoral actors.

Second, Technology Acceptance Theory (Davis, 1989) and its extensions inform the analysis of public readiness to embrace blockchain-based electoral systems. Davis's model identifies perceived usefulness and perceived ease of use as the primary determinants of technology adoption. In the electoral context, perceived usefulness corresponds to public confidence that the technology will produce fairer outcomes; perceived ease of use relates to the accessibility of the voting interface for a diverse electorate with varying levels of digital literacy. Survey data from Igwebuike (2023) provides direct evidence on both dimensions.

METHODOLOGY

This article adopts a mixed-methods approach, integrating quantitative survey research with a technical systems analysis. The primary empirical source is a nationwide survey conducted by Igwebuike (2023) across all 36 Nigerian states and the Federal Capital Territory. The study employed a purposive sampling strategy aimed at achieving a minimum of 20 respondents per state, yielding a target sample of 740 responses. The final dataset comprised 800 validated responses, collected through a combination of online questionnaire platforms (SurveyMonkey and Typeform), hard-copy questionnaires distributed in areas with limited internet penetration, and telephone interviews to capture respondents unwilling or unable to engage with digital instruments.

The survey instrument comprised ten open-ended, subjective questions designed to elicit respondents' own characterizations of electoral challenges, attributions of institutional responsibility, and recommendations for reform. This subjective design was deliberate: it avoided leading questions that might artificially inflate responses in any particular direction and instead allowed themes to emerge organically from respondents' expressed views. Responses were subsequently coded and categorised through thematic analysis, with attributions of electoral failure assigned to three primary institutional actors INEC, the government, and the security agencies and their intersections.

The technical component of the research involved the configuration and testing of a Hyperledger Fabric blockchain network integrated with Realand F-G495 biometric authentication devices, RAMS-2980 attendance management software, Python-based log-parsing scripts, and a frontend web application for vote casting.

The system was operationalised in a controlled demonstration environment, and the voting process from biometric authentication through blockchain ledger recording was validated end-to-end. This technical implementation provides the empirical basis for the system architecture and costing analysis presented in Section 6.

The study adheres to the ethical principles of informed consent, data anonymity, and honest reporting. Questionnaire respondents were not required to provide personally identifying information, and the research presents the raw distribution of views without imputing motive or identity to individual responses.

Source Data and Findings

Survey Data and Institutional Perceptions

The survey yielded 800 responses distributed across Nigeria's 36 states and the FCT. Lagos State recorded the highest number of responses (n=50), consistent with its status as the most populous state, while Bayelsa State recorded the lowest (n=10). The distribution broadly correlates with state population density, lending validity to the representativeness of the sample.

Analysis of responses to the first survey question regarding aspects of the electoral process requiring improvement revealed that 64.75% of respondents (n=518) attributed electoral shortcomings primarily to INEC, citing deficiencies in vote implementation, result collation and transmission, transparency, and use of technology. A further 24.5% (n=196) implicated all three institutional actors INEC, government, and security agencies simultaneously, bringing the cumulative proportion identifying INEC as at least partially responsible to approximately 91%.

The second survey question, inviting respondents to rate INEC's performance on a 0–10 scale derived from their own verbal descriptions, yielded a mean score of approximately 1.93 out of 10—a rating corresponding to descriptions such as "weak," "disappointing," or "deceitful." This finding represents an extraordinarily low level of institutional confidence, indicative of what Easton (1975) would characterize as a systemic legitimacy crisis rather than episodic dissatisfaction.

Question 9, which assessed confidence in INEC's ability to conduct elections reflecting the will of the people, produced a mean confidence score of 1.85 out of 10 equivalent to "very low confidence." Notably, many respondents qualified their pessimism with conditional clauses, indicating that confidence could be restored if INEC were genuinely restructured, made independent of executive influence, or replaced by a technology-driven system incapable of human manipulation.

Demand for Technological Reform

Survey responses to questions 3, 5, 7, and 10 consistently surfaced demand for an electronic, tamper-proof, transparent electoral system. Across these questions, approximately 37–51% of respondents explicitly called for technology-based solutions, with responses ranging from generic calls for "electronic voting" to specific references to biometric systems, blockchain, and real-time result broadcasting. One respondent directly named "blockchain technology" as the desired solution (Igwebuike, 2023, Chapter 4).

The analysis of question 4 which sought positive experiences with INEC revealed that 64.88% of respondents (n=519) could identify no positive aspect of the 2023 electoral process. Of those who identified positives, 12.63% (n=101) cited the electronic accreditation system as the sole notable achievement, suggesting that technological innovation, however partial, is recognised and valued by the electorate.

Technical System Architecture

The Hyperledger Fabric system proposed and tested by Igwebuike (2023) integrates the following hardware and software components:

On the hardware side, the system employs Realand F-G495 biometric devices for voter authentication via fingerprint and facial recognition; laptop or desktop computers (minimum 8GB RAM, Windows 10 Pro) as blockchain nodes; Cisco Business 110 Series Ethernet switches to connect up to four biometric devices per node; and CAT6 Ethernet cables for wired connectivity, deliberately avoiding WiFi to mitigate cyber-attack risks.

The software stack includes Hyperledger Fabric for the permissioned blockchain network; RAMS-2980 V1.0 for biometric data management; Python scripts for log parsing and data extraction; Golang as the primary language of the Hyperledger Fabric codebase; Docker and Docker Compose for container management; and a Node.js-based REST API server for frontend-to-blockchain communication.

The voting process in the proposed system proceeds as follows: voters are pre-registered via the Realand F-G495 device, with fingerprint and facial data stored in the RAMS-2980 system; on election day, biometric authentication unlocks a secure web application on the polling station computer; the authenticated voter selects a candidate and submits their vote; the vote is transmitted via REST API to the Hyperledger Fabric network and recorded on the blockchain ledger through smart contract (chaincode) invocation; the web application closes automatically upon vote submission; and all votes are recorded with full auditability on the distributed ledger, accessible to all network participants in real time.

Cost Analysis

Igwebuike (2023) conducted a detailed costing exercise for nationwide deployment across Nigeria's 176,974 polling units, grouped into approximately 44,244 polling stations (4 polling units per station). The estimated hardware costs include:

176,974 Realand F-G495 biometric devices at ₦90,000 each (total: ₦15.93 billion); 44,244 computers at ₦300,000 each (total: ₦13.27 billion); 44,244 Cisco Ethernet switches at ₦12,000 each (total: ₦530.9 million); and CAT6 cable sets at ₦25,000 per station (total: ₦1.11 billion). Total hardware cost: approximately ₦30.84 billion.

Adding personnel costs (ad-hoc staff at ₦30,500 per unit and field supervisors at ₦100,000 per node) totalling approximately ₦9.73 billion, and a logistics and security allocation of ₦50 billion, the total estimated cost is approximately ₦100 billion roughly one quarter of the ₦400 billion expended in the 2023 elections. At the prevailing exchange rate of approximately ₦1,000 to USD$1, this represents an outlay of approximately USD$100 million, compared to the USD$1 billion spent in 2023.

DISCUSSION OF FINDINGS

The findings presented above converge on a single, compelling conclusion: Nigeria's electoral crisis is fundamentally one of institutional trust, and institutional trust cannot be restored through marginal reforms within the existing paradigm. The near-total collapse of public confidence in INEC as evidenced by mean institutional trust scores of below 2 out of 10 reflects not merely dissatisfaction with the 2023 elections but a deeper, structural disenchantment with a system perceived as systematically biased, corruptible, and opaque.

The consistent demand across survey questions for a technology-driven, tamper-proof electoral system reflects an intuitively sound public diagnosis of the problem. Respondents, many of whom lack technical knowledge of blockchain, nonetheless correctly identify the core issue: that any system whose integrity depends on the honesty of individual human actors will inevitably be compromised in a political environment characterised by high stakes, winner-takes-all incentives, and weak accountability mechanisms. Blockchain technology addresses this problem architecturally rather than behaviorally it does not require electoral officials to be honest; it makes dishonesty technically infeasible.

The proposed Hyperledger Fabric system is particularly well-suited to the Nigerian context for several reasons. Its permissioned architecture ensures that only authorized participants' polling station officials, INEC nodes, and designated media observers can access the network, preventing unauthorized interference while enabling real-time public auditing of aggregate results. The biometric authentication layer eliminates multiple-voting fraud, which has historically been a significant source of result inflation in Nigerian elections. The smart contract-enforced single-vote constraint makes it cryptographically impossible for any voter to cast more than one valid ballot. And the distributed ledger architecture eliminates the central collation bottleneck that, in Igwebuike's (2023) analysis, is the primary locus of result manipulation in the current system.

The cost analysis further strengthens the case for adoption. The reduction from approximately ₦400 billion to ₦100 billion a saving of ₦300 billion or roughly USD$300 million is not merely a fiscal efficiency argument but a democratic one. Excessive electoral expenditure creates perverse incentives: the larger the financial investment required to win an election through legitimate means, the greater the incentive to cut costs through fraud. A cheaper, more secure electoral system reduces the financial barriers to democratic participation and diminishes the return on investment in electoral manipulation.

The technical limitations identified in the study warrant candid acknowledgement. The Realand F-G495 device's inability to transmit biometric data in real time via WebSockets necessitated the use of a periodic Excel export-and-parse workaround an inelegant solution that introduces a three-minute lag in the voting-to-blockchain pipeline. This limitation would need to be resolved in any production deployment, either through hardware customisation by the manufacturer or substitution with a device offering native WebSocket support. Similarly, the inability to combine multiple authentication modalities (fingerprint, face, RFID card) in a single

authentication event reduces the system's resistance to identity fraud. Future iterations should incorporate multi-factor authentication as a standard feature.

The concerns raised by Jefferson and Verified Voting (2023) and Specter et al. (2020) regarding cyber vulnerabilities in blockchain voting systems are largely, though not entirely, addressed by the proposed system's design. By restricting voting to supervised, physical polling stations using INEC-owned hardware connected via wired Ethernet rather than WiFi, the system eliminates the remote-voting attack vectors identified in the literature. The system is explicitly not designed for remote or online voting; its scope is limited to the digitalization and decentralization of the on-premises electoral process. This constraint is both technically sound and politically pragmatic for a first-generation deployment.

POLICY IMPLICATIONS AND RECOMMENDATIONS

The findings of this study carry significant implications for electoral policy in Nigeria and, by extension, for other emerging democracies confronting similar institutional challenges. The following recommendations are advanced:

First, the Electoral Act should be amended to provide explicit legal authorization for blockchain-based voting systems. The existing legal framework was designed around paper ballots and does not adequately contemplate the evidentiary status of cryptographically recorded votes or the liability framework for technical failures in a blockchain system. Legislative reform is a precondition for legitimate deployment.

Second, INEC's institutional independence must be constitutionally entrenched. Survey data consistently identified executive influence over INEC particularly the presidential appointment of the commission's chairman as a structural impediment to impartiality. Amending the Constitution to vest the appointment power in the National Assembly, as recommended by several respondents, would reduce the commission's exposure to executive pressure and improve its public credibility, regardless of the technological infrastructure adopted.

Third, a phased pilot programme should be initiated at the local government level, allowing INEC to test the blockchain system in lower-stakes electoral environments before nationwide rollout. Local government elections offer a suitable testing ground given their smaller electorate, more manageable logistics, and lower political intensity. Lessons from pilot deployments should be systematically evaluated and used to refine the technical architecture and operational protocols.

Fourth, the federal government should engage Realand Technology (the manufacturer of the F-G495 device) or equivalent biometric hardware providers to develop election-specific customisations, including real-time WebSocket data transmission, multi-factor authentication output, and ruggedised hardware suited to Nigeria's diverse environmental conditions. These customisations should be developed under a public procurement framework with open technical specifications to avoid vendor lock-in.

Fifth, a comprehensive voter education programme should accompany any technological transition. The literature on technology acceptance consistently identifies perceived ease of use as a determinant of adoption, and Nigeria's diverse electorate includes significant populations with limited digital literacy. Voter education campaigns, particularly in rural and northern states, should prioritise demystifying the voting interface and building confidence in the system's security and fairness.

Sixth, the security architecture of the network should be subject to independent, internationally accredited penetration testing prior to any electoral deployment. The engagement of international cybersecurity firms, alongside domestic academic institutions, would provide both technical assurance and public credibility.

CONCLUSION

Nigeria's electoral crisis is not primarily a crisis of technology it is a crisis of institutional trust, and technology is the most promising available instrument for restoring that trust. The survey evidence presented in this article demonstrates with striking clarity that Nigerian voters have concluded that the existing electoral architecture,

dependent as it is on the discretion and integrity of human officials at every critical juncture, is incapable of delivering credible outcomes. This conclusion is not unreasonable: it is grounded in decades of observed electoral manipulation, broken institutional promises, and the systematic failure of successive reform initiatives to produce durable improvements.

Blockchain technology, and Hyperledger Fabric in particular, offers a technically credible and economically viable pathway out of this impasse. By removing the central collation bottleneck, eliminating paper-based fraud vectors, enforcing single-vote integrity through smart contracts, and providing real-time public auditability through a distributed ledger, the proposed system addresses the precise structural vulnerabilities that Nigerian voters identify as the source of their disenchantment.

The implementation pathway is neither simple nor risk-free. Technical limitations in current biometric hardware, the complexity of Hyperledger Fabric network administration, the challenge of deploying and maintaining over 44,000 blockchain nodes across a geographically vast and infrastructurally uneven country, and the need for legislative reform and institutional restructuring all represent significant obstacles. None of these obstacles, however, is insuperable with adequate political will, fiscal commitment, and technical expertise.

The stakes of continued inaction are high. A democracy in which elections are reliably perceived as fraudulent is not merely an imperfect democracy it is a democracy in name only, one in which political leaders owe their authority not to the people but to the architects of manipulation. Nigeria deserves better. The technology to deliver better electoral governance exists; what remains is the institutional courage to deploy it.

REFERENCES

1. Adejumobi, S. (2007). Elections in Africa: A fading shadow of democracy? International Political Science Review, 21(1), 59–73. https://doi.org/10.1177/0192512100021001004
2. Agbu, O. (2016). Electoral management bodies and democratization in Africa. In O. Agbu (Ed.), Elections and democratization in West Africa: 1990-2009 (pp. 45–78). CODESRIA.
3. Bratton, M. (2008). Vote buying and violence in Nigerian election campaigns. Electoral Studies, 27(4), 621–632. https://doi.org/10.1016/j.electstud.2008.04.013
4. Castillo, M. (2020, November 3). How to track official election results on Ethereum and EOS. Forbes. https://www.forbes.com/sites/michaeldelcastillo/2020/11/03/how-to-track-official-election-results-on-ethereum-and-eos/
5. Cheeseman, N., & Klaas, B. (2018). How to rig an election. Yale University Press.
6. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008
7. Desouza, K. C., & Somvanshi, K. K. (2018, May 30). How blockchain could help improve election transparency. Brookings Institution. https://www.brookings.edu/articles/how-blockchain-could-improve-election-transparency/
8. Easton, D. (1975). A re-assessment of the concept of political support. British Journal of Political Science, 5(4), 435–457. https://doi.org/10.1017/S0007123400008309
9. European Union Election Observation Mission. (2023). European Union Election Observation Mission Nigeria 2023 final report. European External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2023/EU%20EOM%20Nigeria%202023%20Final%20Report%20EN.pdf
10. Igwebuike, A. C. N. (2023). Proposal for the adoption and implementation of blockchain technology in regional and national elections in Nigeria [Capstone project report, Guglielmo Marconi University / Athena Global Education].
11. Jefferson, D., & Verified Voting. (2023). The myth of "secure" blockchain voting. U.S. Vote Foundation. https://www.usvotefoundation.org/sites/default/files/TheMyth_of_Secure_Blockchain_Voting.pdf
12. March, J. G., & Olsen, J. P. (1984). The new institutionalism: Organizational factors in political life. American Political Science Review, 78(3), 734–749. https://doi.org/10.2307/1961840
13. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org. https://bitcoin.org/bitcoin.pdf

14. Norris, P. (2014). Why electoral integrity matters. Cambridge University Press. https://doi.org/10.1017/CBO9781107280861
15. Specter, M. A., Koppel, J., & Weitzner, D. (2020, August). The ballot is busted before the blockchain: A security analysis of Voatz, the first internet voting application used in US federal elections. Proceedings of the 29th USENIX Security Symposium, 1535–1553. https://doi.org/10.1145/3386554
16. Vinnakota, R. (2021, January 22). Which countries are casting votes using blockchain? HackerNoon. https://hackernoon.com/which-countries-are-casting-votes-using-blockchain-o85b3yh4