Jagua Publication

*Computational Methods, 2(2):13–22, 2025. DOI: 10.58614/cm223*

**Computational Methods**

*Journal homepage: https://www.jpub.org/journal-details.php?journal-id=43*


***Research Article***

# A Proof-of-Concept Architecture for A Blockchain-Based Electoral System for Nigeria

**Uwakmfonabasi Ette[1], Israel Sylvester Umana[1], Bliss Utibe-Abasi Stephen[1*], Philip Asuquo[1], Godwin Chukwukaeze[1] and Egbaji Wiseman Ike-Ochowo[1]**

[1]*Department of Computer Engineering University of Uyo.*
[*]*Corresponding author: blissstephen@uniuyo.edu.ng*

**Article Info**

***Keywords:*** *Blockchain voting, Nigerian elections, Voter anonymity, OTP authentication, Validator verification, Real-time results, Electoral transparency.*

***Received:*** *30.10.2025;*
***Accepted:*** *12.12.2025;*
***Published:*** *17.12.2025*



**Abstract**

**Background of the study:** Nigeria's electoral process has faced systemic ailments like voter intimidation, stuffing of ballot boxes, results alteration, and collation delays leading to a massive decline in voter turnout over the years.
**Goal of the experiment:** These issues stem primarily from over-centralization of the entire electoral process. Most of the vulnerabilities and issues persisted even after the introduction of electronic voting and result transmission technologies, ranging from technical malfunctions to vulnerability to insider interference and manipulation.
**Method/Experiments carried out:** Our approach to combat some of these issues leverages Hyperledger Fabric's permissioned blockchain with Practical Byzantine Fault Tolerance (PBFT) consensus to ensure electoral transparency while preserving ballot secrecy. For the proposed voting process, we implemented a local proof-of-concept that demonstrates the entire voting process, from voter authentication, which relies on an email-based voter authentication with a One-Time Password (OTP) verification sent to the email. Once authenticated, voters make and confirm their choice, and then the system has their vote anonymized, and the validator nodes verify the vote's legitimacy before permanent on-chain recording.
**Results and Conclusion:** We designed a proof-of-concept that was able to successfully prove that the core architectural principles like immutable vote recording, distributed consensus, vote privacy and real-time result verification were achievable. Although the current implementation is limited to a local setup, it provides a foundation for large-scale deployment that could restore trust in the Nigerian democratic process.

## 1. Introduction

In a democratic nation like Nigeria, elections are a very fundamental component that serves as the primary and only process by which citizens can choose their leaders and help shape the governance of the nation. However, Nigeria's electoral process suffers excessive centralization of electoral control, which has led to recurring irregularities, manipulation, and ineffective administration for a long time. Reports and data from both local and international observers throughout the years have consistently raised concerns about the transparency, trustworthiness, and inclusiveness of Nigeria's election system [1, 2]. Data from the Independent National Electoral Commission (INEC) says that voter turnout in Nigeria has been steadily going down over the past 20 years. In 2003, 69.1% of people voted, but by the 2023 general elections, just 27.1% of people voted, the lowest since Nigeria became a democracy again in 1999 [3]. This steady decline can be traced to the fact that voters do not want to come out and their votes do not count because they also perceive election rigging and a lack of transparency in the

electoral process. Incidents of ballot box snatching, vote buying, underage voting, and result falsification have been documented in multiple election cycles [1]. The opacity of manual collation processes and complete dependence on one body of control leaves Nigeria's elections open to manipulation by a few actors. Around a decade ago, blockchain technology emerged as a viable answer to the age-old problem of electoral integrity, providing what traditional methods have continuously failed to do: immutable transparency. Countries such as Estonia, Switzerland, and Sierra Leone have invested in blockchain-based voting systems, hoping to restore what decades of electoral malfeasance have damaged [4, 5]. The appeal is understandable: blockchain promises to overcome the same flaws that have plagued democratic systems for years. Despite its promise, the reality has been way off. Most blockchain voting platforms have simply duplicated the centralization flaws that they were intended to address, concentrating authority in new ways rather than truly spreading it. Some have limited scalability, making them unsuitable for national elections, whereas others use authentication techniques that are so insufficient that they undermine the entire concept of secure voting. The technology exists, but its execution is frustratingly incomplete. Our work bridges this gap by proposing an architecture that genuinely distributes electoral control across multiple independent institutions. We are presenting a proof-of-concept architecture for blockchain-based voting that leverages the features of a permissioned blockchain, multi-layered authentication, tamper-proof record-keeping, and real-time transparency. Our distributed architecture takes care of one of the most urgent democratic concerns in Nigeria by implementing distributed verification that makes tampering with elections much more difficult to achieve.

With the creation of an open, verifiable, and decentralized democratic processes, the system provides the ground for firmer governance and political stability. Overcoming the electoral problem aids in overcoming the larger governance issues that form the bulk of Nigeria's development problems.

This work aims to design and implement a blockchain-based voting platform that addresses Nigeria's electoral shortcomings by helping to ensure that elections are free, fair, transparent, verifiable, secure, and resistant to manipulation. The work offers the following key contributions to knowledge:

- A decentralized control of the entire electoral process by distributing control across multiple independent peers like universities and NGOs thereby eliminating the risks of a single controlling entity.
- Enhanced transparency by creating auditable vote records so that all stakeholders, like the universities and NGOs can independently verify the electoral process.
- Guaranteed immutability so that once votes are recorded on the blockchain, they cannot be altered or deleted.
- A secure process through consensus by requiring approval from a majority of network participants before any changes to recorded data or functionality of the system are accepted.

The idea is ultimately to ensure that every vote cast is counted accurately, thereby restoring public trust in Nigeria's democratic process. This proof-of-concept is particularly directed towards the core blockchain integration and decentralized record of votes feature of a voting system. The emphasis in that direction is towards demonstrating blockchain technology for secure, transparent, tamper-evident voting via a permissioned network on a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism where the verification is split across various institutions to avoid potential collusion.

The remainder of this paper is structured as follows: Section 2 presents the literature review, highlighting some of the existing electoral systems and their shortcomings. Section 3 describes the methodology for our proposed proof-of-concept, including the development environment, architectural design, administrative controls and implementation details. Section 4 covers system testing, results and evaluation, and insights into how the proof-of-concept performed. Section 5 concludes the work, summarizing key contributions, limitations and outlining recommendations for future research and large-scale deployment.

## 2. Literature Review

The history of voting systems shows the continuous struggle of that societies have when it comes to being able to balance accessibility, security, and legitimacy of electoral processes. The old paper ballot procedures used everywhere for so long had the inclination toward physical evidence but were susceptible to stuffing votes, tampering, and logistical inefficiency [6]. When countires transitioned to the use of electronic voting machines (EVMs), the intention was to make voting more efficient and minimize counting errors, but the centralized control of the software used and inauditable audit trails have jeopardized transparency and fostered tampering [7]. In Nigeria, the adoption of card readers and centralized electronic result transmission modernized elections but did not resolve the core trust issues the people had towards the electoral process [8]. Independent reports continued to report records of voter intimidation, stealing of ballots, and alteration of results [9]. When these issues keep occuring the way they do, the appeal for the need for systems that can offer decentralization, transparency, and tamper resistance is on the rise. It is as a result of issues like these that more recently, blockchain models have emerged that offer decentralization, immutability, and end-to-end verifiability [10, 11]. Implementing blockchain into Nigeria's electoral process is meant to address the long-standing trust issues that citizens have when it comes to elections. The decentralized and immutable nature of blockchain technology has put it as a go-to solution to foster the integrity of elections in the future to a great degree [12]. We chose a permissioned blockchain (Hyperledger Fabric) for our proof-of-concept because, although public (permission less) blockchains such as Ethereum provide transparency through open ledgers, they can expose sensitive voting data through deanonymization techniques [13] while in contrast, private (permissioned) blockchains like Hyperledger Fabric restrict network participation to trusted and authorized entities, offering controlled transparency and confidentiality through features such as channels, private data collections, and endorsement policies while still enabling decentralization [14]. A number of pilot tests have already indicated the use of blockchain in elections. Voatz's platform, tested in West Virginia, USA and offered overseas military voting via a mobile app but came under attack for perceived security risks and centralized management [5]. In Moscow's 2019 municipal election, a blockchain election system was used, but its centralized control of keys rendered it vulnerable to tampering.

The examples provided above as a result of our research, show that despite the abilities of the blockchain, one might yet have these electoral systems controlled by a single authority, undermining the decentralization benefit. We aim to use this proof-of-concept to circumvent this wrong use of the blockchain by using a permissioned multi-validator system where NGOs, universities, civic groups, etc, can collaborate to divide the validation burdens so that coordination attacks are less likely. The consensus mechanisms chosen will control how our proposed multi-validator network agrees on transactions and the state of the ledger.

Permission less blockchain public voting is usually Proof of Work (PoW) or Proof of Stake (PoS) based, which are secure but computationally expensive and susceptible to majority attacks [15]. Hyperledger Fabric employs a modular consensus process such as RAFT or KAFKA to offer performance, fault tolerance, and scalability optimization in permissioned settings [14]. Some blockchain voting researches have the sole reliance on a single central validator, which reduces fault tolerance and exposes the system to coordinated attacks [16]. Other protocols employ consensus but limit validator heterogeneity in such a manner that any minor set of validators can form a cabal and manipulate the electoral process. This work is based on a Practical Byzantine Fault Tolerance (PBFT)-based consensus which has been adapted for application in permissioned networks, and the validators from independent institutions, universities, and NGOs are randomly chosen. In our proposed model, 60% of the validators that are drawn from diverse independent institutions are required to agree in order to seal any action or vote to the ledger. This need gives low latency and high throughput as well as immunity to centralized control, and also makes organized tampering exponentially more difficult, especially in a validator network consisting of a thousand validators. Research on voter authentication provide multi-faceted solutions, ranging from straightforward password-based systems to biometric verification [17]. Biometric solutions, even highly secure, provide massive privacy implications and infrastructure demands, particularly in the poor-resource context.

Research on voter authentication offers multi-faceted solutions, ranging from straightforward biometric verification to advanced systems. However, such mechanisms-especially in poor-resource or developing contexts—carry significant privacy risks and logisical burdens. For instance, biometric voter systems may mitigate registration fraud but also raise concerns about surveillance and weak data protections in emerging democracies [18]. In Estonia, integrating facial recognition into e-voting was deemed technically complex, privacy-invasive, and infeasible without strong regulation and infrastructure [19]. Moreover, research into biometric ID systems in Africa reveals how they can amplify structural injustices, marginalize vulnerable populations, and transform public governance into large-scale surveillance landscapes [20]. This work's proposed VIN + OTP technique takes advantage of the existing Nigeria voter register of Independent National Electoral Commission (INEC) to authenticate eligibility and utilize OTPs to ensure that only the registered voter is the one to be permitted to vote. This combination is cost-effective, two-factor secure, mitigating risks of proxy voting and identity theft. For our proof-of-concept implementation, voter authentication utilizes email addresses and one-time passwords (OTP) to simulate the proposed VIN+OTP mechanism intended for production deployment. While transparency is the foundation of election integrity, it must, however, be balanced against the equally important requirement to maintain voter confidentiality. Practically, most systems have attempted to do both by employing advanced cryptographic methods. Helios Voting, for instance, employs homomorphic encryption in such a manner that ballots remain secret while allowing publicly verifiable results [21]. The bottleneck with these sophisticated solutions is that they rely on the existence of a central authority to handle encryption keys, which relapses into the centralization threats that are being addressed. Several voting systems utilizing structural blockchain have been tested or implemented worldwide, each with a distinct set of features but predominantly lacking in a core area of security, decentralization, or scalability. Voatz (USA) combines a mobile voting app with blockchain back-end tech to facilitate remote voting. Despite combining blockchain, Voatz has been criticized for centralizing the verification of votes and administration of identities, relying too heavily on one administrative agency [5]. This type of design opens the door to insider threat vulnerabilities and the possibility of undetected manipulation. Horizon State (Australia) has operational and community control over blockchain decision-making but is operated by a single entity, so depends on the honesty of that one operator for trust in the outcome of the election [22]. Polys (Russia) has blockchain-based cryptographically verifiable voting but is completely under the control of a single corporate organization [23], and it can single-handedly interfere with the process. Agora Voting [24] and Follow My Vote both developed a blockchain-based online voting platform that allows users to verify their vote on a public ledger and even change it before the polls close, enhancing transparency in real time [25]. Yet, lacking robust decentralization of its administrative processes, the platform still depends on a central authority for identity verification and system governance [26].

This allows choke points where manipulation can occur. In addition to these, Democracy Earth and SecureVote (Australia) seek to make the government more democratic through blockchain but usually require centralized control over identities, collapsing the distributed trust model to a singularity. The Estonian e-Residency ballot system [4] possesses integrity features such as blockchain but is centrally controlled by a government department, and thus the process remains open to policy-controlled tampering. The primary constraint throughout these examples is retention of central control, by single validation authority, central ID control, or through dependence upon a minimum set of reliable maintainers. Transparency is offered via the blockchain layer, yet often impaired within the model of governance. This work addresses these weaknesses by dispersing validator authority among a large, diverse network of institutions like NGOs, universities, and civil organizations, with minimal or no governmental affiliation. With a network of 1,000 validators, for instance, collusion would require convincing more than 600 independent bodies to act maliciously in concert, an effort that is logistically and politically impractical. This significantly raises the cost and complexity of any attempted manipulation, ensuring resilience against both external attacks and internal subversion. Relative to current systems, this work's methodology is unique in its focus on removing single points of control. Although systems such as Voatz, Horizon State, and Polys are more transparent by using blockchain, their inclusion of a central controlling entity renders them vulnerable to the same problems that blockchain is trying to solve. Agora Voting and Follow My Vote are more decentralized but maintain control of management by a select few. Even cryptographically secure encryption in Election Guard is vulnerable to its trusted setup. Validator distribution mechanism in this work is exactly what prevents it from being manipulated or controlled by a single individual or a small group of people. This is governance-by diverse-institutions, upheld by studies such as [27, 28], which stress the dissemination of decision-making power for integrity protection in blockchain governance systems. In addition, unlike all the other works that are based on blanket user credentials or single-step ID authentication, this work uses a VIN + OTP authentication procedure. This procedure not only authenticates that any individual voter is an actual registrant in the Nigerian electoral roll but also authenticates that they are an active voter through one-time code posted to their registered contact. This securely removes impersonation attacks, which have tainted common and blockchain elections throughout the globe. By combining a permissioned blockchain platform, a PBFT-based consensus protocol, and a context-dependent, multi-layered voter authentication scheme, this work establishes a robust, unambiguous, and tamper-evident electoral process. By bringing distributed trust, context-dependent authentication, and consensus integrity together, this work is more secure and contextually relevant to Nigeria than the majority of its global counterparts.

# 3. Methodology

## 3.1. Development and Deployment Environment

The development of our voting system implements a local proof-of-concept to validate our proposed architectural design for distributed blockchain-based voting. We used JavaScript as the basis of the implementation, as it provides the ability to interact with Hyperledger Fabric SDK. We used Visual Studio Code (VS Code) to code the codebase owing to the feature-rich debugging, terminal, and Docker and Fabric-extension support. Docker formed the basis for containerizing the elements of the Fabric network as this current implementation run entirely on a single develeopment machine using containerized Hyperledger Fabric components such as the network peers, orderers, and certificate authorities to simulate a multi-node network environment.

## 3.2. Consensus Mechanism Analysis

The proof-of-concept we designed makes use of Practical Byzantine Fault Tolerance (PBFT) consensus, mainly because it ensures fast final results and strong security both of which are crucial for fair and reliable elections. PBFT also offers several benefits that make it well-suited for voting systems:

- **Byzantine Fault Tolerance:** During our research, we realised that PBFT can tolerate up to $f = \frac{(n-1)}{3}$ Byzantine failures, where n = the total number of validators. For large-scale development of our proof-of-concept, we proposed a 1,000+validator network which translates to resilience against up to 333+ compromised nodes, providing really good security against coordinated attacks.
- **Deterministic Finality:** Unlike other consensus mechanisms that only give probability of confirmation, PBFT provides an immediate transaction finality once a consensus in the network is reached. This takes away waiting time, doubt and guarantees that every submitted vote is permanently and securely recorded on the blockchain.
- **Performance Characteristics:** PBFT usually has a 0 $n^2$ message complexity, but modern versions use smarter communication and message grouping techniques to reduce this load. Our proposed architecture uses a 60% + consensus threshold which aligns with PBFT's standard 67% requirement.
- **Scalability Considerations:** For large-scale deployment, we propose strategic validator placement across Nigeria' telecommunications infrastructure to minimise network latency and further optimize performance during peak voting periods.

## 3.3. Network and Transaction Data Flow

In this system, the voting process begins when a registered voter accesses the platform, they begin with an email-based authentication that requires an OTP sent to that mail. This approach simulates the proposed production-scale VIN+OTP authentication mechanism while still maintaining the security principles required for electoral integrity. After the voter is authenticated, the voter is able to choose a running election and his favorite candidate. This choice is then encoded as a blockchain transaction but prior to the system adding an anonymization layer over it which removes any personally identifiable information. This anonymized transaction, is then passed through the JSON-RPC gateway, which serves as a secure interface between the voter application and the Hyperledger Fabric network is frontend to Fabric network communication. After this, the transaction then follows Fabric's execute-order-validate pattern where it is first sent to endorsing peers, who endorse it to the chaincode logic checking voter eligibility, ensuring no vote duplication, and whether the election has not been closed. After the endorsements reach network consensus (e.g., 60% agreement among validator peers), the transaction is submitted to the ordering service. It gets ordered with other transactions and packaged in a block. The committing peers then endorse the block based on endorsement policies and commit the new, immutable vote record to the ledger. The architectural flow is represented in Figure 1 and 2.

In a production-grade deployment, the same would be done on 1,000+ peers spread across standalone institutions such as NGOs, universities, and civic groups. This decentralized architecture means that nobody including electoral commissions can manipulate or control votes.

## 3.4. Identity Management and Privacy Protection

In electoral systems, identity verification is non-negotiable, yet it must be balanced with an equally critical requirement, preserving the secrecy of the ballot. The identification management layer of the system does this weighing through certificate-based authentication and an in-house developed anonymization module. Every participant, voter, administrator, or validator peer, is issued an X.509 digital certificate that is uniquely signed by the Hyperledger Fabric Certificate Authority (CA). The certificates are cryptographically secured to the participant's private key, allowing secure authentication without exporting sensitive credentials over the network. In our current implementation, voters certificate authority is pre-generated and associated with email address to simulate the distributed certificate authority structure planned for production-grade deployment. When the users (voter or admin) complete their email and OTP verification, the system retrieves the corresponding X.509 certificate, which grants network access with the appropriate role permissions. Our proof-of-concept design demonstrates how production deployment will integrate national voter databases for automated certificate authority generation while still maintaining the security properties of distributed trust There is a place for the anonymization module before the voting transaction enters the blockchain life cycle. It plays two roles:

- **Stripping Identifiers:** It deletes any explicit identifiers (e.g., certificate subject names or voter IDs) from the transaction data.
- **Vote Encapsulation:** It encapsulates the candidate choice in a structure indistinguishable from other voters' choice structure, resulting in homogeneity of data structure.

This implies that validator peers who validate transactions know an eligible voter has cast a vote but don't have any idea who choice of candidate is. The mechanism ensures separation of duties between recording votes and identity verification:

- Identity verification happens off-chain during the authentication phase. Recording votes happens on-chain with no connection to the individual voter's identity.

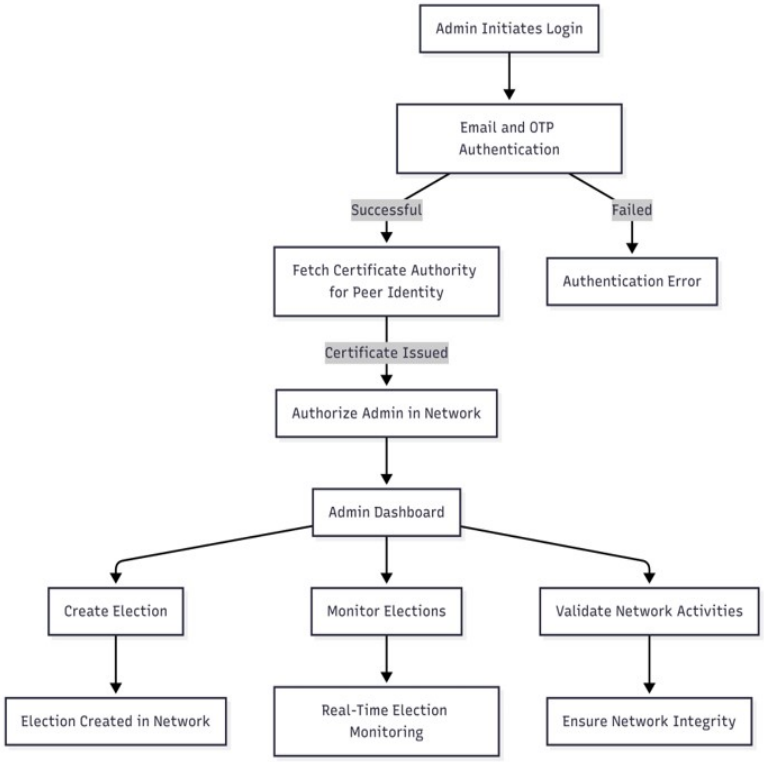


**Figure 1:** Admins Architectural flow

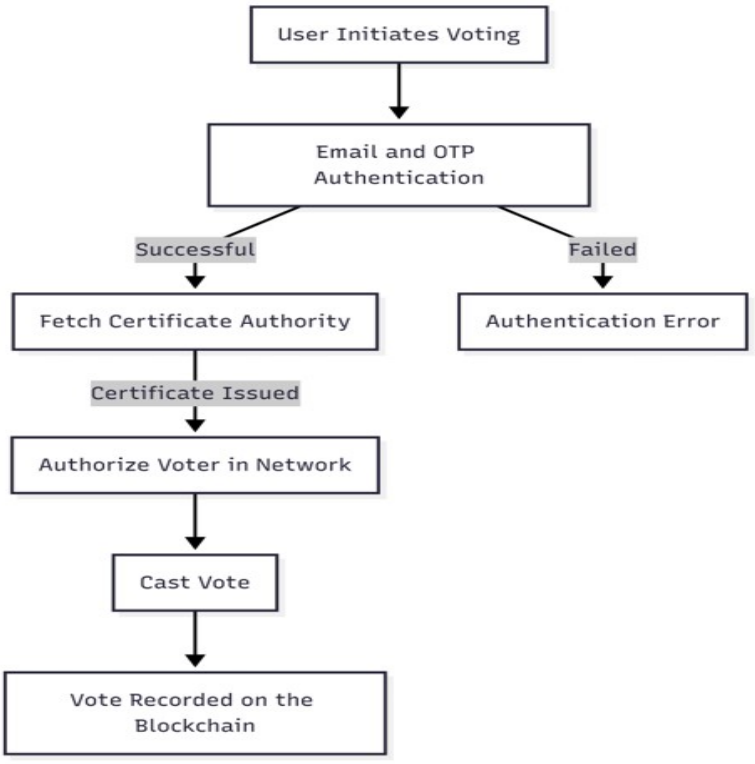


**Figure 2:** Voters Architectural flow

This separation is critical to the prevention of selective transaction rejection, a danger in centralized e-voting systems in which governments can reject votes based on political allegiance. Here, validators see nothing but cryptographically signed, anonymous transactions that are endorsed according to the endorsement policy.

### 3.5. Administrative Controls and Consensus Safeguards

While blockchain provides a secure and immutable background, electoral process also requires an effective tool for performing elections from start to finish. That function in this work is the responsibility of the administrative level, which can be reached by a specified Admin DApp. Admin DApp provides a controlled access platform for running election life cycles where responsible bodies may:

- Create new elections with configurable parameters like start and end dates, candidate lists, and details for qualifications.
- Manage contestants, like adding, editing, or removing entries before an election begins.
- Open and close voting periods, with the security that votes only get cast in the time frame dedicated.
- Construct and publish outcomes, in the assurance that the published outcome is identical to the unchangeable record in the ledger.

But. In contrast to traditional systems where a single administrator or election commission would get its voice, all administrative decisions and vote casting inclusive all fall under Hyperledger Fabric endorsement policies here. This means before an administrative decision is completed, it must be endorsed by an independently agreed number. To facilitate this proof-of-concept, there was 60% validator consensus. For manufacturing deployment, this would be over 1,000 geographically distributed peers, controlled by a mix of government, civil society, academia, and world observers. This distributed control makes tampering realistically impossible without an insane level of conspiracy.

The administrative workflow operation is similar to a vote transaction.

- **Proposal Creation:** A step is triggered by the administrator through the Admin DApp that creates a signed proposal.
- **Endorsement:** Validators peer sends a message to endorse for checking if the person who initiated the proposal has the required permissions and if the proposal action complies with election rules.
- **Ordering and Commitment:** The proposal action is then ordered into a block and committed within the ledger only when the transaction has attained the minimum number of independent peers required to be endorsed.

By implementing the consensus requirement for all administrative actions, we prevent any single administrator from controlling election outcomes. This ensures that electoral legitimacy comes from the distributed network, not an individual authority.

### 3.6. Implementation Achievements

Our proof-of-concept successfully proved that voting using a blockchain-based system can indeed bring the degree of transparency, security, and privacy guarantee that is well required in present-day election processes in Nigeria without offering much complications to the user. In practice, our framework was able to demonstrate that election results could have their trust transferred from a single central source to an open collection of honest, non-conspiratorial peers, with everyone having the same copy of the electoral ledger. We were able to achieve the following at this stage of development:

- **Immutable Record of Vote:** Once a vote was cast and recorded, it could not be deleted or updated, making post-election tampering impossible.
- **Consensus-Based Authentication:** All the admin operations and votes casted were authenticated by validator peers, making sure that it is no prone to one-party result manipulation.
- **Privacy Protection:** The anonymization module successfully eliminated all personally identifiable information prior to a vote being able to reach the validator network. This blinds validators to who a voter voted for, eliminating recommending or vote suppression bias.
- **Smooth Frontend–Blockchain Interface:** With the wallet integration via browser extension, JSON-RPC gateway, and DApps specially designed for that purpose, the voters have the ability to utilize the system like they use any other contemporary web application without having a single idea about blockchain technology.
- **End-to-End Election Life Cycle Management:** The admin UI offered full control over election configuration, candidate man-agement, voting schedules, and result harvesting governed by the same decentralized consensus rules for voting transactions.

## 4. System Testing, Results and Evaluation

### 4.1. Test Deployment Overview

When testing our designed proof-of-concept, we simulated an end-to-end election cycle from initial election setup and candidate registration to vote casting, and then monitoring of results by the admins using a scaled down Hyperledger Fabric network that maintained all of the key features of a production environment. Our test environment included:

- The Hyperledger Fabric Network
- **Voter DApp:** The web interface where the voters will cast their votes.
- **Admin DApp:** Here, admins create the elections, add candidates, manage election stages, and tally votes.
- **JSON-RPC Gateway:** This serves as the bridge between the blockchain network and DApps to facilitate secure and reliable exchange of messages.

All the interactions we carried out followed the standard Fabric transaction flow from proposal submission, to peer endorsement, ordering, and finally ledger commitment.

## 4.2. Functional Testing and Validation

### Administrative Controls

We began testing the administrative controls from election management that is, from the Admin DApp, we created elections by defining the necessary parameters (title, description, start/end time) and adding the candidates. All admin operations were subject to the same agreement criteria as those of the voters' operation.

**Key Points:**

- The updates were made available to the validator peers in real-time for vote and the elections were real time only when the predetermined majority of approvals were made.
- Even the admins were not able to change the state of elections individually, but consent validation was required for each lifecycle event (start and end).

**Outcome:** The administrative controls were carried out as expected while maintaining democratic safeguards, but permitting management features that were needed.

### Voter's Authentication

For the voter's authentication process, each of the emails has a certificate-based identity attached to it, which is fetched when the voter inputs their email and OTP. This certificate-based identity is fetched and authorized, granting this voter access to the network.

**Key Observation:**

- With the certificate-based identities, we were able to prove that only unique and legitimate users were allowed on the network.

**Outcome:** Only voters who had the certificate-based identity were authorized to participate in the network.

### Vote Casting

When voters cast their votes, their choice of candidate was anonymized and those votes were sent to validator peers, and then committed to the ledger following Fabric's execute-order-validate pattern.

**Key Observation:**

- Each vote submitted had to be approved by peers before being committed to the ledger.
- All voters were unable to vote twice.
- Validators could not know who the voters voted for due to the anonymization module. This ensured ballot secrecy

**Outcome:** As users cast their votes, it met all privacy requirements while maintaining user-friendly performance characteristics.

## 4.3. Security and Privacy Assessment

Security testing focused on preventing meddling with the electoral process and protecting voter anonymity. The integrity of cryptography, consensus security, and privacy protection were all tested.

### Vote Integrity

The identity system of the framework, certificate-based, authenticated that only valid participants were voting. Every transaction contained a digital signature that was cryptographically verified prior to any blocks being written into it. Pre-lead ledger, replay attacks on previous transactions or unsigned requests were denied.

### Voter Privacy

The module anonymized the vote by stripping away the identifying information prior to its receipt from the validators. It eliminated selective endorsement on the basis of candidate preference while maintaining the same amount of secrecy as in-person polling booths, without compromising on digital verifiability.

### Cryptographic Security

The browser wallet extension provided additional protection by maintaining user control over private keys throughout the transaction process. Keys never left the extension environment, reducing exposure to potential front-end attacks and ensuring that cryptographic security remained under voter control.

## 4.4. Overall System Evaluation

The proof-of-concept successfully validated the core principles of blockchain-based democratic participation. This comprehensive system's architectural comparison between our proof-of-concept and existing implementations as seen in Table 1 reveals a number of significant advantages in validator distribution and consensus mechanisms. Our design choices translate into measurably superior security properties as

**Table 1:** Comparative Analysis of Blockchain Voting Systems Architecture

| System | Blockchain Type | Validators/ Nodes | Consensus Mechanism | Validator Distribution | Authentication Method | Voter Privacy Method |
|---|---|---|---|---|---|---|
| Voatz [26] | Permissioned (Hyperledger Fabric) | 32 | Custom modified | AWS and Azure (centralized cloud) | Biometric (facial recognition + ID) | Backend encryption (admin access) |
| Helios [21] | None (Centralized server) | 1 (single trustee) | N/A (single server) | Single central server | Email + password | Homomorphic encryption |
| Estonian eResidency [4] | Permissioned | Unknown | Unknown | Government controlled | National ID card | Government managed |
| Proposed PoC | Permissioned (Hyperledger Fabric) | 1,000+ | PBFT (60% threshold) | Multiple independent institutions (NGOs, universities) | VIN + OTP | Anonymization module + Certificate based |

**Table 2:** Security Properties Comparison

| Security Property | Proposed PoC | Voatz | Helios |
|---|---|---|---|
| Decentralized Control | Full | Partial | None |
| Transparency | Full | Partial | Full |
| Consensus Security | PBFT (60%) | Proprietary | N/A |
| Voter Privacy | Cryptographic + Anonymization | Bäckend controlled | Homomorphic encryption |
| Coercion Resistance | Anonymization | Backend vulnerable | Partial |
| Independent Verification | Any stakeholder | Limited access | Public audit |
| Admin Access Control | Consensus based | Centralized | Single admin |

seen in Table 2, particularly in decentralization, consensus security, and voter privacy. The threat resistance analysis as shown in Table 3 demonstrates resilience against insider manipulation, result tampering, and vote deanonymization vulnerabilities that continue to plague both traditional and existing blockchain-based electoral systems. This approach to electoral systems successfully proved that a decentralized electoral infrastructure can provide election integrity while still preserving voter privacy and preventing institutional manipulation.

### Objective Achievement Assessment

The test confirmed that the foundational architecture is secure and resilient enough to handle real electoral processes. Security functionalities, including ballot anonymization and certificate-based authentication, functioned flawlessly throughout testing. The system provided open and transparent audit trails without compromising single voter anonymity, overcoming existing weaknesses of electronic voting systems. Consensus mechanisms and cryptographic principles offer a solid base for scalability. Distributed trust model elevates electoral security from institutional trust to mathematical certainty and delivers a new model of democratic participation in which electoral legitimacy is based on mathematical certainty rather than institutional trust.

**Table 3:** Threat Model Resistance Analysis

| Attack Vector | Proposed PoC | Voatz | Helios | Traditional Systems |
|---|---|---|---|---|
| Single Point of Failure | Resistant (1,000+ nodes) | Vulnerable (32 nodes, 2 cloud providers) | Highly Vulnerable (1 server) | Highly Vulnerable |
| Insider Manipulation | Requires 600+ colluding entities | Requires admin access or 17 nodes | Single admin access | Electoral commission access |
| Vote Deanonymization | Cryptographically protected | Vulnerable to admin [7] | Server can deanonymize [6] | Manual collation exposure |
| Result Tampering | Requires 60% validator collusion | Possible with admin access | Possible with server access | Common vulnerability |
| Network Partition | Fault tolerant (PBFT) | Limited tolerance | Not applicable | Not applicable |
| Coercion/Vote Buying | Anonymization verification | Receipt enables verification | Audit enables verification | Polling booth protected |

## 5. Conclusion

The successful proof-of-concept shows that blockchain-based voting systems can offer security and transparency without giving up the democratic principles necessary for valid electoral processes. The proof-of-concept achieved all the primary objectives of decentralization, transparency, immutability, consensus security, and voter choice anonymity were all met. However, if this proof-of-concept was to get to production level, it would involve extensive work in infrastructure scaling, identity management, user experience design, and operational automation. The distributed trust paradigm tested in our proof-of-concept sets out a realistic process towards elections that are not only transparent and secure but are by design resistant to the manipulation that has plagued democratic institutions for so long. For future work, we recommend large-scale deployment, which will require cloud infrastructure with auto-scaling capabilities and CDN-hosted delivery to ensure reliable performance while eliminating all single points of failure through mirrored gateways. Also, in order to achieve performance optimization, we suggest that peer synchronization and network latency must be addressed to maintain responsiveness during peak voting periods. Production deployment also demands comprehensive automation including backend orchestration, automated vote counting and result publication, along with standardized disaster recovery and validator management protocols for coordinating hundreds of independent institutional participants.

### Article Information

**Conflict of Interest:** The authors confirm that there were no conflicts of interests.

**Disclaimer (Artificial Intelligence):** The author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.), and text-to-image generators have been used during writing or editing of manuscripts.

**Competing Interests:** Authors have declared that no competing interests exist.

## References

[1] European Union Election Observation Mission. Nigeria 2019 eu eom final report. Technical report, 2019.

[2] National Democratic Institute. Iri/ndi international election observation mission to nigeria final report of the 2023 general election. Technical report, 2023.

[3] Independent National Electoral Commission. Report of the 2023 general election. Technical report, 2024.

[4] S. Heiberg, T. Martens, P. Vinkel, and J. Willemson. Improving the verifiability of the estonian internet voting scheme. In *Proceedings of the International Conference for Electronic Voting E-Vote-ID 2016. Springer International Publishing, October*. Springer International Publishing, October 2016.

[5] M. A. Specter, J. Koppel, and D. Weitzner. The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in u.s. federal elections. In *29th USENIX Security Symposium (USENIX Security 20). USENIX Association, 2020*, 2020.

[6] D. M. Sommer, M. Schneider, J. Gut, and S. Capkun. Cyber-risks in paper voting. arXiv preprint, 2020.

[7] Brennan Center for Justice. Voting machines at risk in 2022. Technical report, 2022.

[8] H. A. Idowu. Biometric technologies and the prospect of sustainable democracy in africa, journal = Journal of African Elections. 20(1): 23–43, 2021.

[9] Yiaga Africa. Election manipulation risk index (emri) iii. Technical report, May 2023.

[10] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. arXiv preprint, July 2018.

[11] P. Noizat. Blockchain electronic vote. In *Handbook of Digital Currency*, pages 453–461. Elsevier Inc, 2015.

[12] S. Chouhan and D. G. Sharma. A new era of elections: Leveraging blockchain for fair and transparent voting. arXiv preprint, 2025.

[13] F. B´eres, I. A. Seres, M. Quintyne-Collins, and A. A. Benczu´r. Blockchain is watching you: Profiling and deanonymizing ethereum users. arXiv preprint, 2020.

[14] E. Androulaki, C. Cachin, A. De Caro, and E. Kokoris-Kogias. Channels: Horizontal scaling and confidentiality on permissioned blockchains with application on hyperledger fabric. Technical report, Écolecole Polytechnique Fédérale de Lausanne, 2018.

[15] I. A. A´lvarez, V. Gramlich, and J. Sedlmeir. Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake. arXiv preprint, January 2024.

[16] H. Jayasooriya, D. Bandara, N. Hemachandra, N. Kuruwitaarachchi, and S. Kahandawala. Sbft: A scalable and decentralized trust infrastructure. Conference proceedings: ICEBE 2022, 2018.

[17] H. Hamran, M. Abdullah, M. E. Naveed, and A. R. Afzal. Design and implementation of secure electronic voting system using fingerprint biometrics. *Journal of Artificial Intelligence and Computing*, 1(1):1–5, 2023. ISSN (p): 3005-3358.

[18] R. King. Biometric voter enrollment engenders rewards and risks. Biometric Update, April 2014.

[19] Republic of. Estonia Information System Authority. The implementation of biometrics in e-voting requires prolonged testing, July 2021.

[20] K. Wodajo. Societal and structural risks of biometric id: Towards people's right to privacy. *Sage Journals*, 29(4):614–631, 2024.

[21] Ben Adida. Helios: Web-based open-audit voting. In *USENIX Security Symposium*. 2008.

[22] I. Allen and M. Allen. Blockchain shareholder voting: A hard fork for 21st-century corporate governance. *Penn Law Journal*, 21(2): 405–440, 2019.

[23] M. H. Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl. Blockchain-based e-voting systems: A technology review. 2023.

[24] D. P. De Filippi, D. M. Mannan, S. Cossar, T. Merk, and J. Kamalova. Blockchain technology and polycentric governance. Technical report, European University Institute, 2024.

[25] A. Swiffen. How blockchain-based voting could save democracy. Democracy Chronicles, October 2018.

[26] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa. *E-voting meets blockchain: A survey*. IEEE Access, 2023.

[27] S. Ølnes, J. Ubacht, and M. Janssen. Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, 34(3):355–364, 2017.

[28] M. Pilkington. Blockchain technology: principles and applications. In Research Handbook on Digital Transfor-mations, editor, *Edward Elgar Publishing*, chapter 11. 2016.