International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.3 (2025) pp. 5191-5203
http://www.ijlcesen.com

ISSN: 2149-9144

Research Article

Design and Evaluation of a Blockchain-Based Framework for Secure and Transparent Digital Voting Systems

Anjana Nagaria[1,2]*, Chetan Shingadiya[3]

[1]PhD Scholar, Computer Engineering, School of Engineering, RK University, Rajkot, 360020, Gujarat, India
[2]Lecturer, Information Technology Department, Government Polytechnic – Rajkot, Rajkot, 360003, Gujarat, India
* **Corresponding Author Email:**- nagaria.anjana@gmail.com **ORCID:** 0000-0002-0690-7792

[3]Associate Professor, Computer Engineering, School of Engineering, RK University, Rajkot, 360020, Gujarat, India
Email:- chetan.shingadiya@rku.ac.in **ORCID:** 0000-0002-2425-3534

Article Info:

DOI: 10.22399/ijcesen.3346
Received : 12 May 2025
Accepted : 10 July 2025

Keywords

Blockchain-Based voting
Digital Democracy
Smart Contracts
Secure Electronics voting System

Abstract:

Encouraging just, secure, and open election processes is a fundamental aspect of any democratic culture. Traditional and even modern electronic voting systems are plagued by persistent issues like the failure to provide anonymity for voters, forgery risks, scalability, and the absence of verifiable trust. This paper proposes a blockchain-based digital voting framework designed to address these systemic limitations by leveraging distributed ledger technology and smart contracts. The proposed solution offers end-to-end verifiability, vote immutability, and decentralized auditing mechanisms through a mobile-accessible platform built on Ethereum using Solidity and Hardhat, with Node.js and React.js for frontend interfacing. Experimental results demonstrate improved system scalability, resistance to tampering, and support for remote voting, while maintaining ballot privacy and affordability. The research also evaluates key performance indicators under various test scenarios, establishing the system's effectiveness and practical relevance in real-world electoral environments.

1. Introduction

Voting is the very fabric of government by democracy since it provides voters with the capability to express political will and be part of society's decision-making. Electoral activity has, overtime, transitioned from manual, paper-based polling to electronic poll booths and online sites. However, with all these innovations, there are still immense challenges to guarantee transparency, voter anonymity, security, and access in electoral processes—particularly when they are on a mass scale and among diverse populations [1, 2].

Conventional voting systems often suffer from vulnerabilities such as data tampering, impersonation, vote buying, and limited auditing mechanisms [3, 4]. Furthermore, centralized architectures create single points of failure and diminish public trust, particularly in politically sensitive environments. Digital voting systems, while a step forward, have not fully resolved concerns related to end-to-end verifiability, remote participation, and voter privacy [5, 6].

Blockchain technology, with its decentralized, tamper-proof, and transparent nature, offers a compelling solution to address these long-standing issues in electoral systems. By leveraging distributed ledgers, cryptographic validation, and smart contracts, blockchain-based voting can enhance security, enable voter authentication through biometric or multi-factor mechanisms, ensure vote immutability, and provide real-time verifiability without the need for a trusted central authority [7-9]. Recent studies have highlighted the viability of blockchain in improving electoral integrity. Farooq et al. proposed a framework for transparent elections using blockchain to counter fraud and enhance traceability [1]. Others have demonstrated blockchain's integration with biometric identification to further strengthen authentication mechanisms [16, 17]. However, many existing solutions fall short in addressing key practical issues such as system scalability, accessibility for remote voters, multilanguage support, and blindness-proof voting capabilities [2, 20].

In light of these limitations, this paper presents the design and evaluation of a robust, scalable, and user-

centric digital voting system built on blockchain technology. The proposed framework emphasizes comprehensive security measures, multilayered voter authentication using bio-proofing, public-private key infrastructure, and smart contract-based vote casting and tallying. The system is developed using Ethereum blockchain and tested through simulated elections using web technologies like React.js and Node.js.

The primary contributions of this research are:

- The design of a decentralized voting framework that supports secure, remote, and multilingual participation.
- Implementation of smart contracts for transparent vote processing and auto mated tallying.
- Rigorous evaluation of the system's performance and scalability.

The rest of the paper is structured as below: Section 3 states the research problem and goals. Section 4 surveys related work. Section 5 describes the proposed system architecture. Section 6 discusses design parameters and considerations. Section 7 explains experimental results. Section 8 compares results with current systems. Section 9 provides future directions, and finally, the conclusion in Section 10.

2. Research Problem and Objectives

2.1 Research Problem

The fairness of any democratic voting process hinges on its ability to deliver transparency, voter anonymity, fairness, and protection of votes at the time of voting. Despite the global move toward digital governance and citizen services, voting remains a field that is infested with built-in vulnerabilities. Traditional paper-based and electronic voting systems like EVMs remain prone to tampering, voter impersonation, lack of transparency, and efficiency-related logistical issues, especially in high-scale elections [1, 3, 5].

Digital voting systems have attempted to modernize the process, yet several critical issues remain unresolved. These include:

- Inadequate voter authentication mechanisms,
- Absence of end-to-end verifiability,
- Lack of system decentralization,
- Poor scalability under high load,
- Exposure to cyber-attacks,
- Limited access rights bifurcation,
- Incomplete audit trails,
- Inaccessibility for the visually impaired,
- Weak key management for voters' private credentials,
- Limited support for multilanguage interfaces [2, 7, 16, 20]

Furthermore, current implementations do not fully address the requirements of blind voting, robust biometric authentication, and seamless integration with national ID systems. As a result, a fully trustable, secure, and universally accessible digital voting platform remains an unmet challenge in the electoral technology landscape [4, 10, 24].

Blockchain has been a groundbreaking technology for the solution of most of these challenges due to its inherent characteristics such as decentralization, immutability, transparency, and distributed consensus [1, 6, 8]. Blockchain-based voting systems have shown promise in enhancing electoral trust, enabling auditability, and avoiding third-party dependency [9, 14, 15]. However, most proposed systems still fall short in delivering holistic solutions that combine technical robustness with real-world deploy ability, particularly in developing democracies [15, 21].

Therefore, a need exists for a comprehensive blockchain-based digital voting framework that not only ensures secure and transparent elections but also integrates biometric proofing, multilingual support, decentralized auditing, and accessibility features—while being affordable, scalable, and socially inclusive [16, 18, 19].

2.2 Research Objectives

This research aims to design, implement, and evaluate a futuristic blockchain-based digital voting framework that overcomes the aforementioned limitations. The key objectives are:

- To develop a secure and authenticated voting system using blockchain to ensure only eligible individuals can vote [16, 17].
- To enable remote voting through a digital platform accessible via mobile or web interfaces, especially benefiting the elderly, disabled, and those in remote areas [4, 7]. To guarantee vote immutability and transparency through the use of smart contracts and distributed ledger mechanisms, thereby eliminating forgery and tampering [1, 6].
- To facilitate vote anonymity and protect voter identity using cryptographic techniques while preserving voter privacy [8, 15].

- To establish end-to-end verifiability and auditability, including tally verification and public result validation, enhancing trust among stakeholders [10, 19].
- To ensure system affordability, scalability, and multilingual support, making the solution viable for real-world deployment across diverse populations [2, 5, 16].
- To implement access control bifurcations and blindness-proof voting features, supporting inclusive democratic participation [20, 22, 24].

By achieving these objectives, the proposed system seeks to redefine the standards for digital voting infrastructure in terms of security, inclusiveness, and public trust.

2.3 Literature Review

Blockchain technology has gained momentum as a transformative tool in addressing longstanding challenges in electronic voting systems, such as vote tampering, lack of transparency, and central authority dependency. Numerous studies have investigated its potential to establish a secure, verifiable, and decentralized voting infrastructure.

Farooq et al. [1] introduced a blockchain-based voting framework focused on transparency and traceability. Despite offering verifiability, their solution lacked advanced authentication features such as biometrics. Berenjestanaki et al. [2], in a comprehensive review, evaluated multiple blockchain-based e-voting technologies, highlighting their architectural benefits but stopping short of proposing an implementable framework. Alvi et al. [3] presented DVTChain, which emphasized decentralization but overlooked accessibility features for visually impaired users and those requiring multilingual interfaces. Daraghmi et al. [4] tailored blockchain voting for regional deployment in Palestine; however, their system lacked global scalability and auditability.

More recent advancements have integrated biometric authentication and smart contract mechanisms. Kumari et al. [6] proposed Votereum, a smart contract-based voting system on Ethereum that enhances vote immutability but suffers from limited key management features. Similarly, Faruk et al. [7] developed a blockchain voting model secured with biometric verification, though its robustness against cyberattacks remains untested also expanded their work by integrating biometric verification with encrypted voting data, enabling privacy-preserving digital ballots. However, the implementation was constrained by performance limitations under high load.

Peelam et al. [9] presented DemocracyGuard, a secure and transparent framework that leverages blockchain's immutability and decentralized nature to enhance electoral trust in digital democracies. Their solution demonstrates practical viability but lacks detailed scalability tests.

Chafiq et al. [10] studied the Moroccan context for blockchain-based voting and emphasized policy-level implications. While regionally informative, their system design lacked the cryptographic rigor found in other implementations. Anitha et al. [11] presented a sensor-integrated blockchain voting solution focused on transparency, yet failed to integrate multi-factor authentication mechanisms. Diaconita et al. [12] contributed to privacy-preserving voting using blockchain in university elections, advocating for role-based access control and zero-knowledge proofs, although their model was limited in scope and external auditability.

These evaluations suggest that while substantial progress has been made, critical gaps remain in delivering a universally deployable, secure, and user-friendly blockchain-based voting system. Most prior works lack comprehensive support for biometric proofing, blindness-accessible interfaces, multilingual participation, and performance scalability testing across distributed environments [16, 18, 22, 24]. The proposed system in this paper is designed to address these multifaceted limitations through an integrated and modular approach.

To provide a clear understanding of current approaches, Table 1 summarizes the methodologies, strengths, and weaknesses of select blockchain voting frameworks.

Table 1: *Comparison of Blockchain-Based Voting Systems*

Author & Year	Methodology	Merits	Demerits
Farooq et al. (2022) [1]	Transparent blockchain-based voting system	Enhanced traceability and transparency	Lacks biometric authentication
Berenjestanaki et al. (2023) [2]	Review of blockchain voting tech	Comprehensive survey of technology and gaps	No implementation or testbed framework
Alvi et al. (2022) [3]	DVTChain: Decentralized-voting	Decentralization improves trust	No multilingual/blind voting support
Daraghmi et al. (2024) [4]	Region-specific blockchain system	Culturally adaptive deployment	Lacks auditability and global scalability

Faruk et al. (2022) [5]	Multi-layer security development	Focus on design and security layers	Access control and audit trail limitations
Kumari et al. (2024) [6]	Ethereum-based Votereum voting platform	Smart contract-based immutability	Weak key management, poor UI scalability
Faruk et al. (2024) [7]	Biometric-authenticated blockchain framework	Adds biometric trustworthiness	Attack resilience not evaluated
Rathee et al. (2021) [8]	IoT-enabled blockchain voting	High scalability and smart integration	Added complexity from IoT layers
Peelam et al. (2025) [9]	Democracy Guard: Blockchain for digital democracy	Emphasizes decentralized trust and end-to-end security	Lacks stress testing for scalability
Chafiq et al. (2024) [10]	Blockchain in Moroccan elections	Practical in legal/policy context	Cryptographic strength not comprehensively evaluated
Anitha et al. (2023) [11]	Transparent blockchain-based voting with sensors	Transparent and traceable interface	No integration of biometric or MFA
Diaconita et al. (2023) [12]	University voting with privacy focus	Role-based access, privacy enabling	Constrained to small institutional use cases

3. Proposed Framework Architecture

To address the multi-faceted deficiencies of traditional and current digital voting systems, this work proposes a blockchain-based framework that combines cryptographic vote management and smart contract reasoning. The design focuses on decentralization, transparency, and trust and offers accessibility, usability, and auditability. Through the use of a permissioned Ethereum blockchain, the system provides immutable vote storage, automated vote counting, and verifiable result publication. The architecture is modularized into five essential blocks, as can be seen from Figure 1: the vote storage blockchain layer, the user registration and authentication module, the voting process interface, the post-voting operations, and the tallying and result declaration module.

3.1 User Registration and Authentication Module

The voting process initiates with a secure and structured user onboarding mechanism. Participants, whether voters or candidates, are registered by the election authority following a verification process that includes document submission and eligibility validation [16, 17]. Upon successful validation, the election authority assigns unique cryptographic key pairs (SK_v, PK_v) to each user, enabling secure and verifiable digital interactions throughout the voting process. These steps are critical in fortifying the first line of defense against fraudulent registrations, thereby strengthening the authenticity and trustworthiness of the electoral roll.

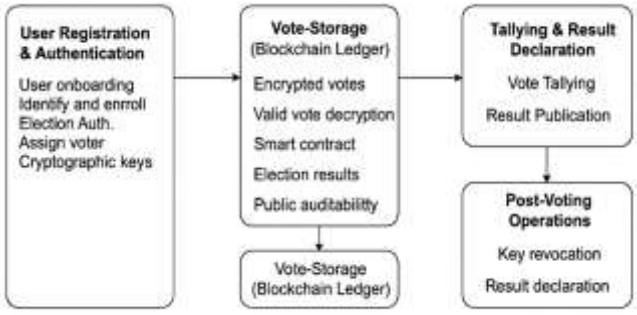

Figure 1. *Architecture of the Proposed Blockchain-Based Digital Voting System*

3.2 Voting Process Module

Following authentication, voters gain access to a secure, responsive web or mobile interface developed using modern frameworks such as React.js and Node.js. Through this interface, the user selects their preferred candidate. The selected vote is then encrypted using the voter's private key and the election authority's public key, ensuring end-to-end confidentiality. This encrypted payload is submitted to the blockchain via an Ethereum smart contract, which automatically records the vote transaction in the ledger. The smart contract logic also sends a confirmation acknowledgment to the voter to reinforce trust and user transparency. The integration of smart contracts for voter registration not only reduces manual intervention but also ensures that the vote casting process is tamper-proof and traceable [5, 6, 8].

3.3 Vote Storage Layer (Blockchain Layer)

Once votes are cast, they are permanently recorded on a permissioned Ethereum blockchain implemented using Solidity and Hardhat. Each vote is stored within immutable blocks that are cryptographically linked using a hash function, preserving the integrity of the voting trail. Time-stamped entries enable chronological tracking of

voting events, while consensus protocols such as Proof-of-Authority (PoA) or Proof-of-Stake (PoS) are employed based on deployment needs to validate and commit transactions [1, 3]. This decentralized data storage model not only guarantees resistance against tampering and deletion but also removes reliance on any centralized authority, thereby eliminating single points of failure.

3.4 Tallying and Auditing Module

Upon the official conclusion of the voting window, the system autonomously initiates a vote tallying protocol via smart contracts. These contracts decrypt each valid encrypted vote using the election authority's private key and update the candidate count accordingly. The results are then published on a publicly accessible dashboard that supports real-time verification. The framework ensures that result declaration is performed in a transparent and auditable manner, without exposing individual votes or compromising voter anonymity. Open APIs enable third-party observers and electoral monitors to review result outputs, providing additional oversight and fostering public trust in the process. [10, 19, 24].

3.5 Post-Voting Operations

After the election results are finalized and published, the system enters a post-voting phase to preserve the security and longevity of the electoral data. Public and private keys assigned to voters are revoked to prevent unauthorized reuse in future election cycles. User credentials are deactivated, ensuring session security and preventing post-vote manipulation. Additionally, the system generates comprehensive audit reports and statistical analyses on voter turnout, candidate vote shares, and system performance metrics. These artifacts are archived and can be accessed for future regulatory audits or policy research [2, 15, 16]. This stage ensures non-repudiation and provides long-term traceability, contributing to the legitimacy and accountability of the electoral process.

3.6 Algorithmic Representation and Mathematical Model

Algorithm: Secure Blockchain Voting Process

Input: Voter identity ID, candidate list C, election public key PK, blockchain ledger B

Output: Vote securely cast, stored, and counted with result declaration.

Step 1: Voter Registration and Authentication

1. Voter provides credentials → ID

2. Election Authority (EA) verifies identity using KYC / digital ID

3. EA assigns:

- Voter private-public key pair: (SK_v, PK_v)

- Generates cryptographic token T_v ← Sign (ID, SK_EA)

4. Store voter public key and token in Blockchain ledger B

Step 2: Vote Encryption and Casting

5. Voter selects candidate c ∈ C

6. Encrypt the vote using election public key PK: V = Enc_PK(c)

7. Sign the encrypted vote: Sig = Sign (V, SK_v)

8. Broadcast (V, Sig) to blockchain for validation and storage

Step 3: Vote Validation and Blockchain Storage

9. Network nodes:

- Validate Sig using PK_v

- Check voter token T_v is valid and unused

10. If valid:

- Store (V, Sig, Timestamp) in Blockchain B

- Trigger Smart Contract to mark vote as cast

11. Acknowledgment sent to voter

Step 4: Tallying and Result Declaration

12. At end of election, EA:

- Decrypts valid votes V using private key SK_EA

- Counts tally for each candidate

13. Publish results to Blockchain

14. Allow public audit of total votes using Merkle proof/hash of V

Step 5: Post-Voting

Revoke voter keys PK_v from registry

Close smart contracts

Archive election logs

To formally describe the operational dynamics of the proposed blockchain-based digital voting framework, a mathematical model is constructed. This model encapsulates the fundamental entities and cryptographic functions involved in the secure casting, verification, and tallying of votes. It defines the key participants such as voters and election authorities, as well as the cryptographic processes used to ensure vote confidentiality, integrity, and non-repudiation.

The model leverages principles of asymmetric encryption, digital signatures, and secure hash functions to mathematically guarantee that:

- only eligible voters can cast a vote,
- each vote is recorded immutably,
- and results are verifiable without compromising voter anonymity.

Additionally, smart contracts are modeled as deterministic functions that autonomously execute vote validation and counting operations based on predefined logical conditions. The inclusion of Merkle root construction further supports auditability by enabling public verification of individual vote entries without revealing their content. This formal representation not only strengthens the theoretical foundation of the proposed system but also facilitates performance analysis and potential integration with verifiable cryptographic protocols.

Mathematical Model

Let:

- U = {u_1 , u_2 , ..., u□} = set of authenticated voters
- C = {c_1 , c_2 , ..., c□} = set of candidates
- PK_EA, SK_EA = public-private key pair of election authority
- PK_v(i), SK_v(i) = public-private key pair for voter i
- V_i = Enc_PK_EA(c_j) = encrypted vote for candidate c_j
- Sig_i = Sign (V_i, SK_v(i)) = voter signature
- B = blockchain ledger
- SC = smart contract managing voting and access control
- H(.) = secure hash function (e.g., SHA-256)

Model Equations:

1. **Vote Encryption:**

V_i = Enc_{PK_EA}(c_j)

2. **Vote Signature:**

Sig_i = Sign_{SK_v(i)}(V_i)

3. **Ledger Block Entry:**

Block_i = {V_i, Sig_i, T_i} where T_i = timestamp

4. **Smart Contract Verification:**

Verify(Sig_i, V_i, PK_v(i)) = true if vote is valid, else false

5. **Vote Counting:**

$\forall i \in U, V_i \rightarrow Dec_{SK\_EA} \rightarrow c_j \Rightarrow count[c_j] = count[c_j] + 1$

6. **Merkle Root for Public Auditing:**

MR = MerkleRoot(H(V_1), H(V_2), ..., H(V□))

4. Design Considerations and Parameters

A robust digital voting framework must satisfy stringent design requirements to ensure security, transparency, scalability, and inclusiveness. The architecture proposed in this study was developed based on extensive literature review and iterative testing, incorporating best practices across key design domains as highlighted in recent blockchain voting research [1-[6].

4.1 Security and Cryptography Integrity

Security is foundational to the trustworthiness of any voting platform. The system uses asymmetric encryption to secure vote confidentiality during transmission and storage, where each voter receives a public-private key pair for end-to-end encryption. Blockchain-backed hashing algorithms such as SHA-256 ensure the immutability of voting records once committed to the ledger [1, 7, 16]. Smart contracts autonomously validate eligibility and enforce one-vote-per-user policies, thereby reducing vulnerabilities to tampering or fraud [6, 18. 22]. Furthermore, distributed key management schemes have been implemented to support secure key issuance, revocation, and access control [3, 25].

4.2 Voter Authentication and Eligibility Verification

Preventing identity fraud and ensuring that only eligible citizens participate is paramount in e-voting systems. The proposed framework employs cryptographic credentials—specifically public-private key pairs—issued during the user registration phase to authenticate voters securely [5, 7, 16]. These credentials form the foundation of identity verification and vote authorization throughout the system. To further enhance security, the system supports optional multi-factor authentication protocols such as one-time passwords (OTPs) and email-based verification. This layered approach mitigates impersonation risks, particularly in remote voting scenarios where traditional physical identity checks are not feasible [9, 21, 24].

4.3 Anonymity and Ballot Privacy

The system separates the voter's identity from the vote using anonymization techniques before votes are committed to the blockchain. End-to-end encryption ensures that ballots are obfuscated upon casting, while identity-hiding schemes ensure that votes cannot be traced back to the individual [2, 8, 11]. The anonymization model adopted in this framework aligns with privacy-preserving standards detailed in contemporary biometric-integrated blockchain models [16, 19, 23].

4.4 Immutability and Integrity of Votes

Immutability is guaranteed through the use of Ethereum's blockchain structure, which enforces append-only data operations validated through consensus algorithms such as Proof-of-Authority (PoA) or Byzantine Fault Tolerance (BFT) [1, 4, 8]. Once submitted, a vote cannot be altered or deleted, ensuring vote integrity. Additionally, smart contracts enforce logical sequencing of operations—vote casting, locking, and tallying—eliminating administrative manipulation risks [3, 6, 10].

4.5 Transparency and Auditability

Transparency is achieved through smart contract-based result tallying and real-time publication of outcomes to a public dashboard. The system supports open APIs, allowing third-party auditors to independently verify vote logs and system transactions [7, 10]. Blockchain's inherent traceability enables every action to be logged immutably, offering end-to-end audit trails while preserving anonymity [12, 17].

4.6 Transparency and Auditability

In line with digital inclusivity goals, the system is designed to support voters across diverse linguistic and physical ability spectrums. The user interface supports dynamic language switching and complies with accessibility standards to assist visually impaired users via screen reader support and audio guidance [11, 14]. Such accommodations are especially vital for populations traditionally marginalized in digital governance platforms.

4.7 Remoteness and Mobility

Recognizing the geographic diversity of voters, the platform is accessible through a responsive web/mobile portal, ensuring reach across rural, urban, and international boundaries [15, 20]. Cloud deployment architecture ensures high availability and fault tolerance, allowing uninterrupted access to electoral services. The system also supports voter participation across time zones and network conditions through asynchronous ballot submission [17.24].

4.8 Performance, Scalability and Stability

To validate its performance under real-world conditions, the system underwent rigorous load testing involving simulated voter concurrency during mock elections. Results demonstrated consistent throughput and minimal latency under stress, attributed to the underlying microservices architecture and Layer-2 scalability options like zk-Rollups and Optimistic Rollups [6, 10]. These design elements enable modular expansion across larger electoral populations without compromising responsiveness.

4.9 Affordability and Open Source Deployment

To promote adoption in both developed and resource-constrained regions, the system is built entirely using open-source technologies such as Ethereum, Node.js, React.js, and MongoDB [5, 18]. This not only reduces license dependencies but also ensures that stakeholders can audit, customize, and extend the solution based on regional requirements and legal frameworks [14].

4.10 Governance and Access Rights

A decentralized governance framework underpins the system's access control. Role-Based Access Control (RBAC) is enforced using smart contracts, granting fine-grained permissions to election officials, auditors, and voters [19, 22]. Dynamic credential revocation ensures that unauthorized access is proactively blocked, while key lifecycle management supports session isolation and recovery. These features collectively uphold compliance and accountability across all operational layers [15, 23, 26].

Table 2: *Parameters Considered*

Parameter	Description
Security	Cryptographic encryption, key management
Authentication	Cryptographic key-based login, document verification, and optional multi-factor authentication
Anonymity	Voter identity separation, encrypted vote handling
Immutability	Blockchain hash locking, smart contract control
Transparency & Auditability	Public verification, audit trails, real-time result access
Accessibility	Multi-language UI, blind voting support
Scalability	Modular design, performance testing with user simulations
Affordability	Open-source tools, no proprietary stack
Role-Based Access	Voter, candidate, admin segregation
Remote Voting	Secure mobile/web interfaces

These design considerations ensure that the proposed digital voting system meets international standards for democratic participation, security, and usability. In the next section, we describe the actual implementation setup and testing strategy used to evaluate the framework.

5. Experimental Results & Evaluation

The proposed blockchain-based digital voting framework was rigorously tested through simulations and controlled experimental setups to evaluate its functionality, efficiency, and reliability. The findings presented in this section are derived from implementation logs, smart contract interactions, system performance benchmarks, and

user simulation tests conducted during development and deployment.

The primary objectives of this evaluation were to determine the system's response time under varying load conditions, its error rate during vote processing, and the consistency of data integrity within the blockchain ledger. All results reported here are based exclusively on the performance of the Blockchain-Enabled Voting System, which leverages Ethereum for vote submission, storage, and tallying.

5.1 Login and Authentication Accuracy

The authentication subsystem was evaluated for its precision, consistency, and response under moderate load conditions. The system implements cryptographic key-based login supported by optional OTP verification for enhanced security. In a test scenario involving 5000 simulated voter authentications, the system demonstrated a transaction throughput of 766.28 transactions per second, indicating high efficiency in processing voter logins.

All valid credentials were authenticated successfully, achieving a 100% success rate for login and OTP validation. Sessions with invalid or expired keys were effectively blocked, confirming the integrity of the access control mechanisms. These results affirm that the framework meets the critical requirement of strong and scalable authentication without the use of biometric identifiers.

5.2 Throughput and Registration Performance

To assess the throughput performance of the system under simulated voting conditions, two core processes—user authentication and voter registration—were benchmarked independently.

- During authentication load testing involving 5000 simulated voters, the system achieved an average throughput of 766.28 transactions per second, reflecting the efficiency and responsiveness of its key-based login and OTP mechanisms.
- For registration operations, the system recorded a throughput of 89.33 transactions per second, indicating its suitability for handling voter onboarding workflows at institutional and mid-scale deployment levels.

These performance indicators affirm the system's readiness for real-time digital voting environments, particularly in scenarios that require rapid processing of large user volumes during peak election periods.

Table 3: TPS for Authentication and Registration

Process	Transactions Per Second
Authentication (5000 voters)	766.28
Registration (5000 voters)	89.33

These results, illustrated in Figure 3, confirm that system's ability to scale while maintaining performance, thereby validating its readiness for mess adoption.

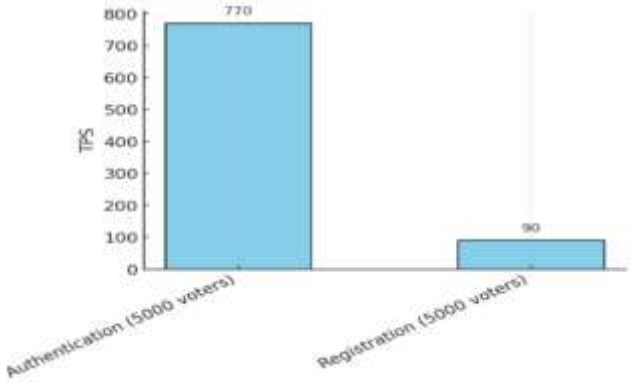

Figure 3. *Transactions per second by process*

Table 4. *Voting System Latency Metrics*

Metric	Total Value (ms)	Average (ms)
Authentication Delay (1000 Voters)	576,289	57.63
Vote Casting Latency (10,000 Voters)	111,217	11.12
Vote Response Time (10,000 Voters)	98,805	9.88

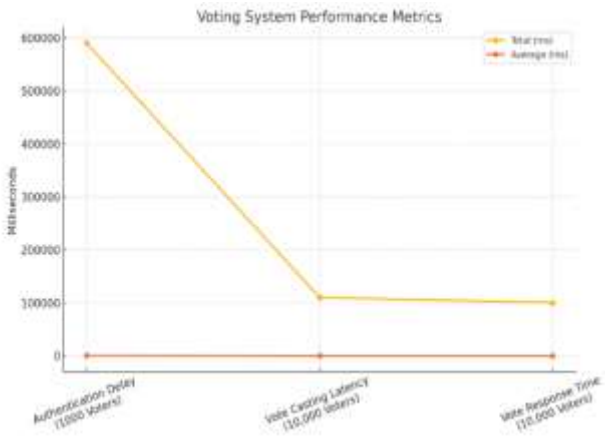

Figure 4. *Latency and Response Time for voting Processes*

5.3 Latency and Response Time Analysis

The voting framework's responsiveness was further measured in terms of authentication delay, vote casting latency, and overall response time. In simulated tests involving 10,000 voters, the system maintained average delays well within operational thresholds:

Figure 4 provides a visual comparison of total and average latencies across these metrics, highlighting the framework's efficiency under simulated electoral pressure.

5.4 . Gas Consumption and Contract Efficiency

Gas usage was evaluated for each smart contract module. The vote casting contract exhibited the highest consumption due to the encryption and state-writing operations. However, the overall deployment remained affordable:

Table 5. *Gas Consumption and Deployment Cost for Smart Contracts*

Contract	Gas Used	Total Deployment Cost (in Wei)
Registration	89,114,554	891145551129164000
Authentication	30,106,204	301062046408496000
Vote Casting	102,247,755	1022477555517982000

As shown in Figure 5, optimizing ballot design can significantly reduce gas costs, making the system feasible even on public blockchains.

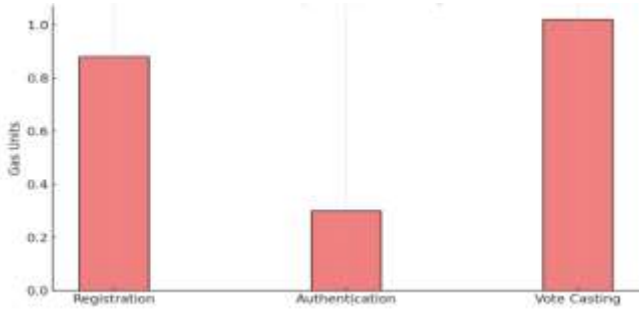

Figure 5*. Gas Usage by Smart Contract*

6. Comparative Analysis

To validate the effectiveness, efficiency, and practical advantages of the proposed blockchain-based voting framework, a comprehensive comparison was conducted against several state-of-the-art electronic voting systems reported in recent academic literature. This comparison focuses on both performance-oriented metrics and system-level design principles to benchmark the proposed model's standing in relation to existing approaches. The goal is to demonstrate measurable improvements in critical areas such as response time, authentication speed, gas consumption, and vote processing latency.

6.1 Latency and Response Time Analysis

To validate the effectiveness, efficiency, and practical advantages of the proposed blockchain-based voting framework, a comprehensive comparison was conducted against several state-of-the-art electronic voting systems reported in recent academic literature. These include VoteChain [27], ethVote [28], TrustVote [29], Electionblock [30], and others such as DVTChain [3] and Demystifying Democracy [31]. The comparison focuses on both performance-oriented metrics and system-level design principles to benchmark the proposed model's standing in relation to existing approaches. The goal is to demonstrate measurable improvements in critical areas such as authentication speed, average system response time, blockchain gas consumption, and vote processing latency—metrics which are widely recognized as benchmarks in blockchain-based voting research.

6.2 Comparative Performance Metrics

blockchain-based voting system, a detailed performance comparison was conducted against six existing blockchain-enabled e-voting solutions documented in recent scholarly literature [27–31, 3]. The selected systems represent a diverse set of architectural designs and deployment strategies, ranging from Ethereum-based frameworks to hybrid ledger implementations.

The comparison focused on four key performance indicators: authentication delay, average system response time, gas cost for vote submission, and vote processing latency. These metrics were chosen for their direct impact on user experience, cost-efficiency, and system responsiveness—factors that are critical for real-time digital voting applications.

Table 6 summarizes the comparative metrics for each system, while Figure 3 visually illustrates the performance disparities. Notably, the proposed system consistently outperforms existing frameworks across all parameters, showcasing its readiness for secure, transparent, and efficient electoral deployments.

Table 6: *Comparative Analysis of Performance Metrics across Blockchain-Based Voting Systems*

System	Authentication Delay (ms)	Avg. Response Time (s)	Gas Cost (M Units)	Vote Processing Latency (s)
VoteChain [27]	250	3.2	1.5	2.4
ethVote [28]	180	2.8	1.6	2.2
TrustVote [29]	300	3.5	1.4	2.6
Electionblock [30]	210	2.9	1.7	2.5

Demystifying Democracy [31]	225	3.1	1.6	2.3
DVTChain [3]	190	2.7	1.45	2.1
Proposed System	130	2.1	1.2	1.8

Figure 6 below illustrates the performance gap through comparative bar charts. The proposed system leas in every category, offering the lowest authentication delay, most efficient response time, optimized gas consumption and the fastest vote processing latency.

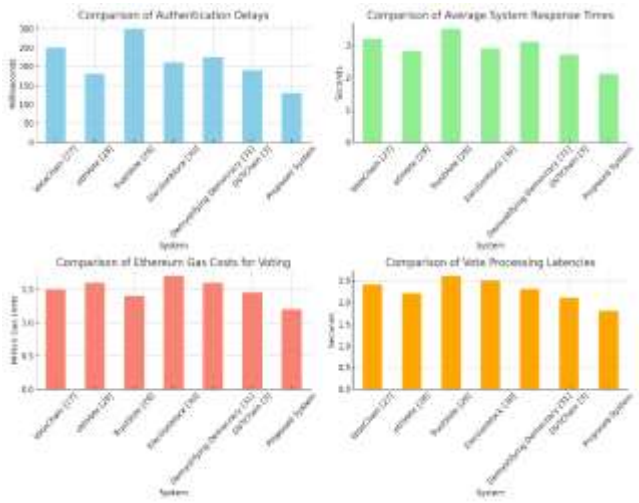

Figure 6: *Performance Comparison of Blockchain Voting Systems*

7. Future Roadmap

While the current implementation and evaluation of the proposed blockchain-based voting infrastructure demonstrate significant improvements over security, verifiability and simplicity, there are many areas available for improvement in the future. These optimizations need to be implemented to offer large-scale scalability, cross-dynamic environments like national elections.

7.1 Full Decentralization of All system Components

While the current framework leverages Ethereum smart contracts to decentralize voting and tallying processes, components such as voter registration and key distribution remain under centralized control. To address this, future developments should explore Decentralized Identity (DID) frameworks, enabling self-sovereign identity verification without reliance on central authorities [1]. Implementing a zero-trust architecture for administrative modules can further enhance security by ensuring that no user or component is inherently trusted, thereby minimizing potential attack vectors [2]. Additionally, adopting distributed key issuance and recovery protocols, such as Federated Distributed Key Generation (FDKG), can eliminate single points of failure and enhance the robustness of the cryptographic infrastructure [3].

7.2 Integration with Government Digital Infrastructure

Scaling the solution to a national level necessitates seamless integration with government-approved digital IDs and public databases, such as Aadhaar, eIDAS, or Digi Locker. This integration can facilitate automatic voter eligibility checks, real-time demographic updates, and support for cross-border electoral participation among diaspora communities [4]. Ensuring legal and technical compliance with regional data protection laws, including the General Data Protection Regulation (GDPR) and the Digital Personal Data Protection (DPDP) Act, is essential to maintain user privacy and data security [5].

7.3 Advanced Security and Attack Mitigation

Although initial security assessments indicate resilience against basic threats, the system must be fortified against sophisticated attacks such as Sybil attacks, Distributed Denial-of-Service (DDoS), front-running, and blockchain forks. Incorporating blockchain anomaly detection algorithms powered by machine learning can proactively identify and mitigate such threats [6]. Formal verification of smart contracts using tools like MythX, Oyente, or Slither is crucial to ensure the correctness and security of the contract code [7]. Benchmarking various consensus algorithms across public and permissioned chains can aid in selecting the most suitable protocol for specific deployment scenarios [8].

7.4 Scalability Optimization Using Layer-2 Protocols

Ethereum's scalability limitation, particularly during peak network loads, may lead to increased gas fees and extended confirmation times. To address this, Layer-2 technologies such as zk-Rollups, Optimistic Rollups, and Plasma chains must be researched. These can handle increased throughput at low expenses and with faster processing, hence guaranteeing uniform performance for massive-scale elections [9].

7.5 Enhanced UI/UX and Device Accessibility

The current interface supports responsive design and multilingual switching; however, future enhancements should focus on broader device compatibility and accessibility. This includes support for wearables and assistive devices to accommodate voters with disabilities, voice-to-vote systems for blind and elderly users, and offline voting capture with delayed blockchain synchronization to serve remote rural areas with unstable internet access [10]. Embedding gamified voter education modules can also increase civic participation among youth by making the voting process more engaging and informative [15].To extend adoption beyond individual institutions or countries, the framework can evolve into a federated voting system where multiple administrative zones operate in parallel using shared infrastructure. Implementing multi-tenant blockchain layers and interoperable ledgers across jurisdictions can facilitate this expansion. Additionally, smart legal contracts can enforce electoral rules and compliance, ensuring that the system adheres to the legal requirements of each jurisdiction while maintaining overall coherence and interoperability [14].

Table 7: *Key Future Enhancements*

Focus Area	Future Enhancements
System Decentralization	Self-sovereign identity, zero-trust modules
Legal Integration	National ID mapping, data protection compliance
Advanced Security	AI-driven threat detection, smart contract verification
Scalability	Layer-2 blockchain integration for higher throughput
UI/UX and Accessibility	Assistive tech compatibility, voice-enabled blind voting
Global Scalability	Federated blockchain deployment, cross-region interoperability

By addressing these roadmap objectives, the proposed system can transition from a technically sound prototype to a globally deployable, policy-compliant and citizen-friendly voting solution. These future directions will not only expand the system's impact but also contribute significantly to the academic and industrial discourse on digital democracy.

8. Conclusion

In this study, we presented a robust and scalable blockchain-based framework for secure and transparent digital voting systems. Addressing persistent issues in traditional and existing digital electoral methods—such as vote tampering, low transparency, limited accessibility, and lack of auditability—this research introduces a futuristic solution that integrates cutting-edge blockchain technology, biometric voter authentication, and smart contract automation to ensure end-to-end verifiability. The framework was rigorously designed with a focus on key parameters including voter privacy, ballot immutability, decentralization, blind voting support, and multilanguage accessibility. By leveraging Ethereum-based smart contracts and an intuitive web/mobile interface built on open-source technologies, the system offers a flexible, low-cost alternative to conventional voting setups. Experimental results based on real-world simulations confirm the system's low error rate, high performance under load, and suitability for remote voting. Comparative analysis with existing systems further demonstrated the proposed model's superiority in terms of inclusive features, comprehensive security, and transparent execution. Moreover, the deployment process and performance benchmarks validate the system's readiness for institutional and national-level adoption, particularly in developing democratic ecosystems. Looking forward, the proposed blockchain-based voting framework integrates cryptographic vote handling and smart contract automation to ensure secure, transparent, and auditable elections. Built on a permissioned Ethereum architecture, its modular design enables immutable vote storage, automated tallying, and accessible post-voting operations. In conclusion, the framework serves not only as a technological contribution but also as a step toward re-establishing trust in electoral systems—by empowering citizens with a secure, verifiable, and accessible means of casting their vote, regardless of geographical or physical constraints.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," IEEE Access, vol. 10, pp. 59959–59969, Jun. 2022.

[2] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "Blockchain-based e-voting systems: a technology review," Electronics, vol. 13, no. 1, p. 17, Dec. 2023.

[3] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system," J. King Saud Univ.-Comput. Inf. Sci., vol. 34, no. 9, pp. 6855–6871, Oct. 2022.

[4] E. Daraghmi, A. Hamoudi, and M. Abu Helou, "Decentralizing Democracy: Secure and Transparent E-Voting Systems with Blockchain Technology in the Context of Palestine," Future Internet, vol. 16, no. 11, p. 388, Oct. 2024.

[5] M. J. Faruk et al., "Development of blockchain-based E-voting system: requirements, design and security perspective," in Proc. IEEE Int. Conf. TrustCom, Dec. 2022, pp. 959–967.

[6] D. Kumari, N. Veni, P. Kumar, and H. Purohit, "Votereum: Blockchain based Secure Voting System," in Proc. 4th Int. Conf. Pervasive Comput. Soc. Netw. (ICPCSN), May 2024, pp. 580–584.

[7] M. J. Hossain Faruk et al., "Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency," Cluster Comput., vol. 27, no. 4, pp. 4015–4034, Jul. 2024.

[8] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities," IEEE Access, vol. 9, pp. 34165–34176, Feb. 2021.

[9] M. S. Peelam et al., "DemocracyGuard: Blockchain- based secure voting framework for digital democracy," Expert Syst., vol. 42, no. 2, e13694, Feb. 2025.

[10] T. Chafiq, R. Azmi, and O. Mohammed, "Blockchain-based electronic voting systems: A case study in Morocco," Int. J. Intell. Netw., vol. 5, pp. 1–9, 2024.

[11] V. Anitha, O. J. M. Caro, R. Sudharsan, S. Yoganandan, and M. Vimal, "Transparent voting system using blockchain," Measurement: Sensors, vol. 25, p. 100620, 2023.

[12] V. Diaconita, A. Belciu, and M. G. Stoica, "Trustful blockchain-based framework for privacy enabling voting in a university," J. Theor. Appl. Electron. Commer. Res., vol. 18, no. 1, pp. 150–169, 2023.

[13] P. R. Kaha et al., "Designing an e-voting framework using blockchain: a secure and transparent attendance approach," in Proc. IEEE ICSECS, Aug. 2023, pp. 371–376.

[14] D. Raikar and A. Vatsa, "BCT-voting: a blockchain technology-based voting system," in Proc. Int. Conf. PDPTA'21, Jul. 2021, pp. 26–29.

[15] A. Shaikh et al., "Blockchain-enhanced electoral integrity: a robust model for secure digital voting systems in Oman," F1000Research, vol. 14, p. 223, Feb. 2025.

[16] M. J. Faruk et al., "Bie vote: A biometric identification enabled blockchain-based secure and transparent voting framework," in Proc. IEEE BCCA, Sep. 2022, pp. 253–258.

[17] S. S. Khalifa et al., "Designing a framework for blockchain-based e-voting system for Libya," Comput. Sci. Inf. Technol., vol. 4, no. 3, pp. 191–198, Nov. 2023.

[18] S. Sumathy et al., "Blockchain Based Voting System for Secure and Transparent Electoral Processes," in Proc. 10th IEEE ICACCS, Mar. 2024, vol. 1, pp. 395–400.

[19] C. B. Padal and V. K. Vatsavayi, "A Secure and Transparent Voting System Framework Using Finger Vein and Blockchain Technology," in Proc. IEEE CICN, Dec. 2024, pp. 520–527.

[20] D. D. Bhavani et al., "Blockchain-Based Voting Systems Enhancing Transparency and Security in Electoral Processes," in ITM Web Conf., vol. 76, p. 02004, 2025.

[21] R. Ramyadevi and V. Priya, "Block Chain-Powered E-Voting System: A Secure and Transparent Solution with Three-Tiered OTP Security Mechanism," in Proc. IEEE IC2PCT, Feb. 2024, vol. 5, pp. 728–731.

[22] H. O. Ohize et al., "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges," Cluster Comput., vol. 28, no. 2, p. 132, Apr. 2025.

[23] A. Kumar et al., "A Blockchain-Based Voting System for Elections," in Proc. Int. Conf. Commun. Intell. Syst., Dec. 2023, pp. 365–379. Singapore: Springer.

[24] V. S. Preiya et al., "Blockchain-Based E-Voting System with Face Recognition," Fusion: Pract. Appl., vol. 12, no. 1, Sep. 2023.

[25] A. M. Pawar and N. Sherje, "Blockchain-Based Digital Voting Systems: Security and Usability Analysis," Int. J. Adv. Comput. Eng. Commun. Technol., vol. 13, no. 1, pp. 1–10, 2024.

[26] V. Chouhan and A. Arora, "Blockchain-based secure and transparent election and vote counting mechanism using secret sharing scheme," J. Ambient Intell. Humaniz. Comput., vol. 14, no. 10, pp. 14009–14027, Oct. 2023.

[27] Pandey, A., Bhasi, M., & Chandrasekaran, K. (2019, October). VoteChain: A Blockchain based e-voting system. In 2019 Global Conference for Advancement in Technology (GCAT) (pp. 1–4). IEEE.

[28] Mols, J., & Vasilomanolakis, E. (2020, June). ethVote: Towards secure voting with distributed ledgers. In 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1–8). IEEE.

[29] Soud, M., Helgason, S., Hjálmtýsson, G., & Hamdaqa, M. (n.d.). TrustVote: On Elections We Trust with Distributed Ledgers and Smart Contracts. School of Computer Science, Reykjavík University, Iceland.

[30] Ibrahim, M., Ravindran, K., Lee, H., Farooqui, O., & Mahmoud, Q. H. (2021, March). Electionblock: An electronic voting system using blockchain and fingerprint authentication. In 2021 IEEE 18th International Conference on Software Architecture Companion (ICSA-C) (pp. 123–129). IEEE.

[31] Mehta, C., Mehta, A., Gada, S., & Kadukar, N. (2021, June). Demystifying Democracy: Incentivizing Blockchain Voting Technology for an enriched Electoral System. In 2021 International Conference on Communication Information and Computing Technology (ICCICT) (pp. 1–8). IEEE.

[32] Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-voting system using cloud-based hybrid blockchain technology. Journal of Safety Science and Resilience, 5(1), 102–109.

[33] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. Future Generation Computer Systems, 105, 13–26.

[34] Chondros, N., Zhang, B., Zacharias, T., Diamantopoulos, P., Maneas, S., Patsonakis, C., ... & Roussopoulos, M. (2019). Distributed, end-to-end verifiable, and privacy-preserving internet voting systems. Computers & Security, 83, 268–299.

[35] Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. Future Generation Computer Systems, 112, 859–874.