A THEORETICAL FRAMEWORK FOR ENSURING INTEGRITY AND TRANSPARENCY IN BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEMS

Ngo Duc Canh[1,*], Chu Thi Quyen[1], Le Thi Linh[1], Roan Van Quyen[1], Phung Thi Thuy[1]

DOI: https://doi.org/10.57001/huih5804.2026.073

ABSTRACT

In the context of digital transformation, electronic voting (e-voting) has become an important trend for improving election efficiency and increasing voter participation. However, traditional centralized e-voting systems still face significant challenges related to transparency, verifiability, and data manipulation risks. This paper proposes a theoretical framework for blockchain-based electronic voting systems to enhance election integrity, transparency, and auditability. The study applies literature analysis and system modeling methods to construct an architectural model consisting of the voter layer, voting layer, blockchain layer, and verification layer. The proposed framework clarifies the role of smart contracts in automating election procedures, enforcing voting rules, and supporting independent verification. In addition, the study discusses practical issues related to gas costs, system performance, and scalability when deploying voting systems on public blockchain networks.

Keywords: *Blockchain, E-voting, Transparency, Integrity, Theoretical Framework, Smart Contract.*

[1]School of Information and Communication Technology, Hanoi University of Industry, VietNam

[*]Email: 2022605692@st.haui.edu.vn

Received: 05/01/2026

Revised: 15/3/2026

Accepted: 30/3/2026

1. INTRODUCTION

In the context of rapid digital transformation, electronic voting (e-voting) has attracted increasing attention as a promising approach for improving electoral efficiency, reducing operational costs, and expanding voter participation [1]. Compared with traditional paper-based elections, e-voting systems offer advantages in terms of automation, result processing speed, and accessibility. However, most currently deployed e-voting platforms are still developed based on centralized client-server architectures, where election data and vote counting processes are controlled by a central authority. Such architectures introduce significant concerns regarding transparency, auditability, and system trustworthiness [2]. Several studies have highlighted the inherent limitations of centralized e-voting systems. Research [3] demonstrated that centralized voting infrastructures are vulnerable to cyberattacks, insider manipulation, and software tampering, while Research [4] emphasized that the absence of independent verification mechanisms undermines voter confidence in election outcomes. Furthermore, the existence of a single point of failure (SPOF) creates risks related to service disruption and unauthorized modification of election data. Although cryptographic techniques such as blind signatures and homomorphic encryption have been introduced to improve ballot privacy and integrity, many traditional e-voting systems still rely on trusted third parties (TTPs), which limits decentralization and independent verifiability [5]. The emergence of blockchain technology has introduced a new paradigm for constructing transparent and tamper-resistant electronic voting systems. Blockchain provides decentralization, immutability, distributed consensus, and public auditability, allowing election data to be recorded in a manner that is resistant to unauthorized modification [3]. In blockchain-based architectures, votes can be stored as transactions on a distributed ledger, where every transaction is validated collectively by network participants. This mechanism reduces dependence on

centralized authorities and enhances trust through verifiable computation rather than institutional control. Recent years have witnessed growing research interest in blockchain-based e-voting systems. Lee et al. [2] proposed an early blockchain voting framework integrating authentication servers and distributed ledgers; however, the system still relied heavily on centralized voter verification mechanisms. McCorry et al. [8] introduced a smart contract-based voting model on Ethereum that enabled public verifiability and decentralized vote tallying. Nevertheless, the model suffered from scalability limitations and high gas consumption due to on-chain computation. Liu and Research [7] later proposed a privacy-preserving blockchain voting scheme using cryptographic commitments to enhance ballot confidentiality, although the complexity of the protocol increased computational overhead and reduced practical deployability. More recent studies between 2022 and 2024 have explored advanced approaches such as zero-knowledge proof (ZKP) voting, rollup-based architectures, decentralized identity (DID), and Layer-2 blockchain integration to improve scalability and privacy [8, 9]. For example, zk-based voting systems provide stronger anonymity guarantees and end-to-end verifiability, while rollup architectures aim to reduce transaction costs and increase throughput on public blockchains. However, these approaches often introduce substantial cryptographic complexity, dependence on additional infrastructure layers, or challenges in practical implementation and usability. In many cases, the proposed systems remain experimental or implementation-oriented without providing a generalized architectural framework that systematically explains how transparency, auditability, voter eligibility, and privacy can be simultaneously guaranteed within a unified e-voting model. Table 1 summarizes several representative blockchain-based e-voting studies and highlights their limitations in terms of scalability, privacy, transparency, and practical deployment. Based on the literature review above, an important research gap can be identified. Existing studies either focus primarily on cryptographic protocol construction or emphasize implementation-specific solutions, while insufficient attention has been paid to establishing a coherent theoretical framework that systematically explains how blockchain architecture, smart contracts, and decentralized verification mechanisms interact to ensure election integrity, transparency, and auditability in large-scale electronic voting systems. In addition, many current approaches do not clearly address the relationship between voter eligibility verification, identity uniqueness, smart contract enforcement, and independent public verification within a unified architectural model. To address this gap, this study proposes a theoretical framework for blockchain-based electronic voting systems that focuses on the architectural integration of blockchain and smart contracts to strengthen transparency, data integrity, and independent verifiability. Unlike previous studies that mainly concentrate on introducing new cryptographic primitives or implementation techniques, this research adopts a system-oriented and conceptual perspective. The proposed framework emphasizes how election rules can be consistently enforced through smart contracts while maintaining auditability and minimizing subjective intervention from centralized authorities. The proposed framework also discusses the role of complementary mechanisms such as commitment-based voting, decentralized identity verification, and distributed data storage in improving election security and trustworthiness. Furthermore, the study analyzes practical challenges related to scalability, gas costs, privacy preservation, and deployment feasibility on public blockchain infrastructures.

The main contributions of this study are:

(1) proposing a theoretical framework for blockchain-based e-voting systems;

(2) developing a conceptual architecture integrating blockchain, smart contracts, and decentralized verification;

(3) analyzing limitations and research gaps in existing blockchain-based voting approaches;

(4) discussing practical deployment challenges and future research directions.

2. BLOCKCHAIN AND SMART CONTRACTS IN VOTIBNG SYSTEM

2.1. Blockchain

The concept of blockchain was initially introduced by Haber and Stornetta in 1991 as a method for timestamping digital documents to prevent unauthorized modification [7]. Since then, blockchain has evolved into a foundational technology for decentralized data management. From a theoretical standpoint, blockchain can be understood as a distributed ledger system in which data are organized into sequentially

connected blocks, with each block cryptographically linked to its predecessor. This structure ensures that any alteration in previously recorded data would invalidate the entire chain, thereby enabling strong guarantees of data integrity.

Two essential characteristics define blockchain systems: decentralization and immutability. Rather than relying on a single controlling entity, the ledger is maintained collectively by a network of nodes operating in a peer-to-peer environment. Data consistency is achieved through consensus mechanisms, which determine the validity of newly added records. Once consensus is reached and a block is appended to the chain, its contents become effectively immutable, meaning they cannot be altered or removed without detection.

Within the theoretical context of electronic voting systems, these properties provide a robust foundation for ensuring both integrity and transparency. By representing each vote as a transaction recorded on the blockchain, the system can enforce the principle that each ballot is uniquely registered and permanently preserved. The immutability of the ledger guarantees that recorded votes cannot be retroactively modified, while its distributed nature allows multiple independent parties to verify the correctness of the election results. Consequently, blockchain enables a shift from trust-based verification toward a model grounded in verifiability and cryptographic assurance.

From a framework-oriented perspective, blockchain serves not merely as a storage mechanism but as an infrastructure that defines how trust, validation, and data consistency are established within the voting system. This makes it a critical component in constructing a theoretical model for secure and transparent electronic elections

2.2. Smart Contracts

Smart contracts extend the capabilities of blockchain by embedding executable logic directly into the distributed ledger. Conceptually, a smart contract is a self-executing program whose rules and conditions are predefined and deployed on the blockchain. Once deployed, these rules operate autonomously and cannot be altered, ensuring that all system behaviors are consistently enforced according to the original design.

From a theoretical perspective, smart contracts play a central role in formalizing and enforcing system-level rules within blockchain-based voting architectures. Instead of relying on external authorities or manual intervention, the execution of voting procedures such as ballot submission, validation, and counting is governed by deterministic code. This guarantees that all participants are subject to the same set of rules, applied uniformly and transparently.

In the context of electronic voting, smart contracts can be interpreted as the mechanism through which core election properties are operationalized. For example, rules related to voter eligibility, vote uniqueness, and result computation can be encoded directly into the contract logic. Because these rules are immutable after deployment, they provide strong assurances that the election process cannot be arbitrarily manipulated. At the same time, the execution of smart contracts is publicly verifiable, allowing external observers to audit the correctness of the process.

Within the proposed theoretical framework, smart contracts are not viewed merely as implementation tools but as formal components that define the behavioral structure of the voting system. They enable the translation of abstract security and transparency requirements into enforceable rules, thereby bridging the gap between conceptual design and system-level guarantees.

3. THEORETICAL FOUNDATIONS

3.1. Requirements of Electronic Voting System

Electronic voting (e-voting) systems must satisfy a set of critical security and operational requirements to ensure fairness, trustworthiness, and legitimacy throughout the electoral process. These requirements have been widely discussed in recent blockchain-based voting studies [1, 4, 6]. However, achieving all requirements simultaneously remains a major challenge, particularly in decentralized and partially untrusted environments. Integrity is considered one of the most fundamental properties of an e-voting system. Every ballot must be accurately recorded and protected against unauthorized modification from the moment it is cast until the final tallying stage. Any alteration of voting data may directly compromise election legitimacy. Recent studies further emphasize that integrity in blockchain-based voting is not limited to data immutability, but also includes verifiable execution of election rules through smart contracts. Transparency and auditability are also essential requirements for modern voting systems. Stakeholders should be able to independently verify election processes and results without relying entirely on

a centralized authority. Recent blockchain-oriented studies increasingly focus on end-to-end verifiability, enabling voters and auditors to validate whether votes are correctly counted while preserving ballot secrecy. This requirement becomes especially important in large-scale elections where public trust is critical. At the same time, voter privacy and anonymity must be preserved to prevent coercion, vote-buying, or voter tracking. Several recent approaches employ advanced cryptographic techniques such as zero-knowledge proofs and homomorphic encryption to strengthen privacy guarantees. Nevertheless, these mechanisms often introduce substantial computational overhead and implementation complexity, limiting their practical deployment on public blockchain infrastructures. Authentication and uniqueness are equally important in preventing unauthorized participation and double voting. Existing studies commonly combine blockchain with decentralized identity (DID), biometric verification, or cryptographic credentials to ensure that each eligible voter can vote only once. However, balancing identity verification with anonymity preservation remains an open challenge in current e-voting research.

Overall, recent literature demonstrates that no existing solution fully satisfies integrity, transparency, scalability, privacy, and efficiency simultaneously. This limitation motivates the need for a more systematic theoretical framework capable of analyzing how blockchain properties can be aligned with the core requirements of electronic voting systems.

3.2. Fundamental Properties of Blockchain Technology

Blockchain technology has attracted considerable attention in electronic voting research due to its decentralized architecture and tamper-resistant data model. Unlike traditional centralized systems, blockchain enables distributed consensus among multiple network participants, thereby reducing dependence on a single trusted authority. Decentralization is particularly important in e-voting because it mitigates the risks associated with single points of failure and centralized manipulation. In public blockchain networks, transaction validation is performed collectively through consensus mechanisms, which increases resistance against unauthorized intervention. Immutability is another critical property. Once voting data is validated and appended to the blockchain ledger, altering previously recorded information becomes computationally impractical. This characteristic strengthens election integrity and enables reliable post-election auditing. Transparency and traceability further distinguish blockchain-based systems from conventional e-voting architectures. Since blockchain transactions are publicly verifiable, election-related operations can be independently inspected and audited. Recent studies increasingly emphasize that transparency should not merely expose voting data, but also provide verifiable evidence that election procedures are executed correctly and consistently. Despite these advantages, recent research also highlights several limitations of blockchain adoption in e-voting systems. Public blockchain platforms often suffer from scalability constraints, transaction latency, and high gas costs during periods of network congestion. Privacy-preserving approaches based on zero-knowledge proofs improve anonymity but substantially increase computational complexity and verification overhead. Meanwhile, private blockchain architectures may improve performance but often sacrifice decentralization and public verifiability.

Consequently, blockchain alone cannot fully solve all challenges of electronic voting. Instead, recent studies suggest that effective e-voting systems require carefully designed architectures that balance transparency, privacy, scalability, and operational feasibility.

3.3. Mapping Between Blockchain Properties and Voting System Requirements

From a theoretical perspective, one of the key challenges in blockchain-based e-voting research lies in systematically aligning blockchain properties with the functional and security requirements of voting systems. While many previous studies discuss these aspects independently, fewer works provide a unified conceptual relationship between them. Blockchain immutability directly supports election integrity by ensuring that once ballots are recorded, they cannot be modified retroactively. The hash-linked structure of blockchain blocks enables the detection of unauthorized tampering attempts and preserves consistency across distributed nodes. Transparency and auditability are strengthened through distributed ledger mechanisms. Since transaction histories remain publicly accessible, independent observers can verify voting activities without relying solely on election authorities. This property contributes significantly to building public trust and reducing opportunities for hidden manipulation. Consensus mechanisms also support rule enforcement by ensuring that only valid transactions are accepted into

the network. In blockchain-based voting systems, this allows election procedures defined within smart contracts to be executed consistently and automatically. However, recent studies indicate that improving one property often introduces trade-offs in another. For example, privacy-enhancing techniques such as zero-knowledge proofs increase computational overhead and verification complexity. Similarly, scalability solutions such as rollup architectures improve throughput but introduce additional infrastructure dependencies and architectural complexity.

These observations indicate that current blockchain-based voting studies still lack a comprehensive theoretical framework capable of systematically explaining how election requirements, blockchain properties, and architectural trade-offs interact within a unified model. Therefore, this study proposes a theoretical framework aimed at clarifying these relationships and providing conceptual guidelines for designing transparent, verifiable, and practically deployable blockchain-based voting systems.

4. PROPOSED THEORETICAL FRAMEWORK

4.1. Conceptual Architecture

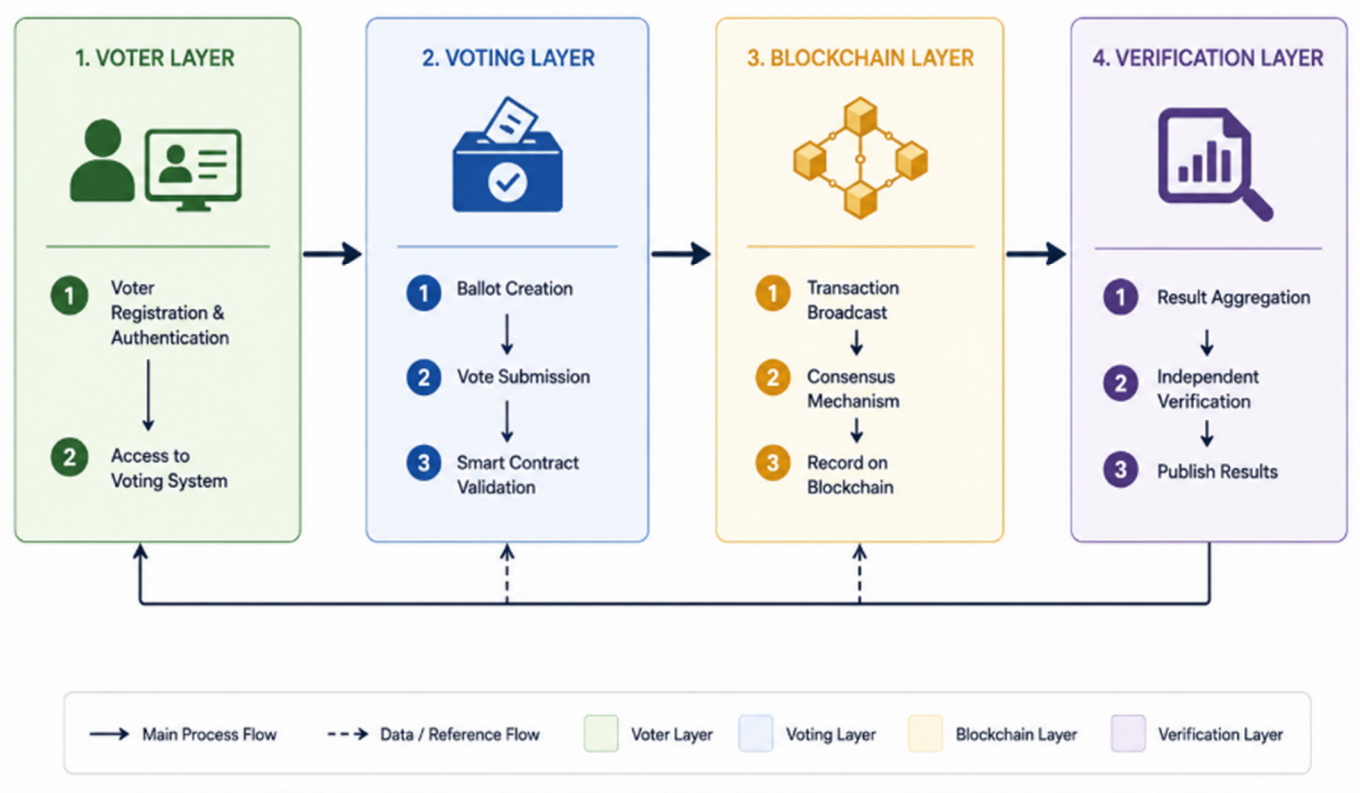

Figure 1. System architecture

This study proposes a theoretical framework for blockchain-based electronic voting systems aimed at systematically connecting election requirements with blockchain properties within a unified conceptual architecture. Unlike many previous studies that mainly focus on cryptographic protocol implementation or isolated voting mechanisms, the proposed framework emphasizes architectural abstraction and logical enforcement of election properties through blockchain and smart contract mechanisms. The novelty of the proposed framework lies not in introducing a new cryptographic primitive, but in providing a unified theoretical abstraction that explains how blockchain properties, smart contract logic, and voting system requirements interact to establish transparency, integrity, auditability, and voter uniqueness within a single conceptual model.

The proposed architecture consists of four primary layers, as illustrated in Figure 1.

- Voter Layer: This layer represents entities participating in the election process. It is responsible for voter authentication, eligibility verification, and identity uniqueness enforcement. The layer ensures that only authorized participants are allowed to interact with the voting system.

- Voting Layer: This layer manages ballot generation, vote submission, and enforcement of election rules. Smart contract logic is conceptually integrated at this

layer to ensure that voting procedures are executed consistently and automatically.

- Blockchain Layer: This layer serves as the distributed infrastructure responsible for transaction validation, immutable storage, and consensus execution. All voting-related transactions are recorded within this layer to ensure integrity and transparency.

- Verification Layer: This layer enables independent auditing and verification of election outcomes. Auditors and external observers can verify voting results through publicly accessible blockchain data without relying on centralized authorities.

The separation of these layers enables the framework to clearly distinguish between participation, rule enforcement, data storage, and verification mechanisms. From a theoretical perspective, blockchain is not treated merely as a storage platform, but as a trust-enabling infrastructure that systematically supports transparency, auditability, and integrity enforcement.

In addition, the framework explicitly models the relationship between blockchain properties and election requirements, allowing the system to be analyzed independently of specific implementation technologies or deployment environments.

4.2. Formalization of Core Security and Correctness Properties

To improve the theoretical rigor of the proposed framework, core election properties are formally represented using mathematical notation. This formalization provides a conceptual basis for analyzing correctness, integrity, and transparency in blockchain-based electronic voting systems.

Let:

$$V = \{v_1, v_2, \ldots, v_n\}$$

be the set of eligible voters,

$$B = \{ b_1, b_2, \ldots, b_m\}$$

be the set of ballots,

$$T = \{ t_1, t_2, \ldots, t_k\}$$

be the set of blockchain transactions, and *C* reqresent the smart contract logic responsible for enforcing election rules.

4.2.1. Integrity Property

The integrity property is formalized as:

$$\forall b_i \in B,\ recorded(b_i) \Rightarrow immutable(b_i)$$

This expression indicates that once a ballot b_i has been successfully recorded on the blockchain, it becomes immutable and cannot be modified without detection.

The property is theoretically supported by the cryptographic structure of blockchain systems:

$$Hash(Block_n) = H(Block_n \parallel Hash(Block_{n-1}))$$

where:

- H denotes a cryptographic hash function,

- $Block_n$ represents the current block,

- $Hash(Block_{n-1})$ is the hash value of the previous block.

This chained structure ensures that any modification to historical voting data changes subsequent hash values, making unauthorized tampering detectable across the network.

From a voting-system perspective, this mechanism guarantees that ballots remain consistent throughout the election lifecycle.

4.2.2. Transparency Property

Transparency is represented as:

$$\forall t_i \in T,\ accessible(t_i) \wedge verifiable(t_i)$$

This condition states that every blockchain transaction related to the election process must remain publicly accessible and independently verifiable. The transparency property enables voters, auditors, and external observers to inspect election-related activities without relying on centralized authorities. In the proposed framework, transparency is treated not merely as data visibility but as the ability to independently validate election correctness through distributed consensus and immutable transaction history.

4.2.3. Uniqueness Property

To prevent double voting, the uniqueness condition is defined as:

$$\forall v_i \in V,\ \exists!\ b_i \in B$$

This expression ensures that each eligible voter can generate exactly one valid ballot during the election process.

Within the proposed framework, this property is conceptually enforced through smart contract execution logic:

$$vote(v_i) = \begin{cases} valid, & \text{if } voted(v_i) = false \\ rejected, & \text{otherwise} \end{cases}$$

This mechanism guarantees that once a voter has submitted a valid ballot, subsequent voting attempts are automatically rejected by the system.

4.2.4. Auditability Property

The auditability property is represented as:

$$\forall r \in R,\ verify(r, T) = true$$

where:

- R denotes the set of published election results,

- T represents the transaction history stored on the blockchain.

This condition ensures that election results can be independently verified using publicly recorded blockchain data. Unlike traditional voting systems where auditing often depends on trusted authorities, the proposed framework enables decentralized verification through immutable transaction records and publicly accessible consensus data.

4.3. Theoretical Voting Process Model

Based on the proposed framework, the electronic voting process is modeled as a sequence of logically connected stages.

Registration Phase: Eligible voters are authenticated and granted permission to participate in the election process. This phase ensures voter legitimacy and prevents unauthorized participation.

Vote Casting Phase: Voters submit ballots through the voting layer. Smart contract logic validates voting conditions, including voter eligibility and uniqueness constraints.

Recording Phase: Validated ballots are transformed into blockchain transactions and appended to the distributed ledger after consensus verification.

Result Aggregation Phase: Valid ballots are aggregated according to predefined election rules to produce final election outcomes.

Verification Phase: Election results are independently verified through blockchain transaction inspection and audit procedures.

Unlike implementation-oriented systems, the proposed process model focuses on logical consistency and conceptual relationships rather than platform-specific execution details.

4.4. Integrity Assurance Mechanisms

The proposed framework ensures system integrity through several interconnected blockchain mechanisms.

Hash-linked Structure: Each block is cryptographically connected to its predecessor through hash references, forming a tamper-evident chain structure.

Immutable Ledger: Once voting transactions are confirmed through consensus, altering previously recorded data becomes computationally impractical.

Distributed Consensus: Consensus mechanisms ensure that only valid transactions are accepted into the blockchain network, thereby preserving data consistency across distributed nodes.

Collectively, these mechanisms establish a theoretical foundation for preventing unauthorized modification of election data.

4.5. Transparency and Auditability Model

Transparency and auditability are treated as central architectural properties within the proposed framework.

Public Verifiability: Blockchain transactions remain publicly accessible, enabling independent verification without requiring centralized trust assumptions.

Independent Auditing: External auditors can verify election correctness by comparing published results against immutable transaction histories.

Traceability: The complete voting history remains permanently recorded, supporting post-election inspection and retrospective auditing.

Unlike traditional voting architectures, transparency in the proposed framework is embedded directly into the system structure rather than added as an external auditing feature.

4.6. Theoretical Result Verification Model

The proposed framework models election result verification based on logical correctness conditions.

Result Publication Condition: Election results are published only after all valid ballots have been successfully recorded and verified.

Hash-based Verification: Aggregated results can be validated against blockchain transaction data through cryptographic verification mechanisms.

Audit Events: Election-related events remain permanently recorded on the blockchain, enabling independent auditing and retrospective verification.

From a theoretical perspective, this model demonstrates how blockchain mechanisms can reduce dependence on centralized trust while improving transparency, auditability, and confidence in election outcomes.

5. DISCUSSION ON PRACTICAL FEASIBILITY

5.1. Deployment Conditions

The practical deployment of blockchain-based electronic voting systems requires several important

conditions related to infrastructure, legal frameworks, and user adoption. From a technological perspective, blockchain networks must provide sufficient scalability and transaction throughput to support large numbers of voters during election periods. Public blockchain platforms offer transparency and decentralization but may face limitations in performance and transaction speed. Therefore, scalability solutions such as Layer-2 architectures can be considered to improve efficiency and reduce congestion. From a legal perspective, blockchain-based voting systems must comply with regulations concerning elections, digital identity, electronic signatures, and personal data protection. The adoption of decentralized verification mechanisms may also require adjustments to existing governance and auditing procedures. In addition, user acceptance plays a critical role in deployment feasibility. Although blockchain improves transparency and auditability, wallet management and transaction confirmation processes may be difficult for non-technical users. Hence, intuitive interfaces and simplified interaction mechanisms are necessary to improve usability and public trust. Compared with existing systems such as Helios or Voatz, the proposed framework focuses more on establishing a generalized theoretical architecture that systematically connects transparency, integrity, uniqueness, and auditability within a unified blockchain-based model.

5.2. Limitations

Despite its advantages, the proposed framework still faces several limitations. First, scalability remains a challenge for public blockchain systems when handling large numbers of voting transactions simultaneously. Second, transaction fees on public blockchains may increase deployment costs, particularly in large-scale elections. Third, although blockchain improves transparency, publicly visible transaction metadata may still raise privacy concerns. Furthermore, the proposed framework is primarily theoretical and focuses on architectural analysis rather than full-scale implementation. Therefore, additional experimental evaluation is necessary to validate the framework in real-world election environments.

5.3. Future Research Directions

Future research may focus on integrating Zero-Knowledge Proofs (ZKP) to improve voter privacy while maintaining verifiability. In addition, Layer-2 scaling solutions such as zk-Rollups may help reduce transaction costs and improve system performance. Another promising direction is the integration of Decentralized Identity (DID) systems to strengthen voter authentication and uniqueness verification while protecting personal information.

Finally, future studies may explore cross-chain voting architectures and DAO-based governance models to improve interoperability, scalability, and decentralization in blockchain-based electronic voting systems.

6. CONCLUSION

This study presents a structured theoretical framework for ensuring integrity and transparency in blockchain-based electronic voting systems. Unlike prior research that focuses on isolated aspects such as cryptographic protocols or system implementations, this work provides a unified model that systematically integrates core election requirements with fundamental blockchain properties. The main theoretical contribution lies in formalizing the relationships between system requirements and decentralized mechanisms, thereby establishing a consistent foundation for analyzing and designing secure e-voting systems. In addition, the proposed framework demonstrates practical applicability by outlining architectural principles and identifying real-world deployment constraints. The validation through case analysis highlights that existing solutions often address individual challenges but lack a comprehensive theoretical structure. By bridging this gap, the proposed framework contributes to advancing the state of research toward more reliable and verifiable voting systems.

Future work will focus on extending the framework through the integration of zero-knowledge proofs for enhanced privacy, Layer-2 solutions for scalability, and decentralized identity systems for robust authentication. Furthermore, empirical validation and quantitative evaluation remain important directions to strengthen the connection between theoretical models and real-world applications.

REFERENCES

[1]. R. Krimmer, D. Duenas-Cid, I. Krivonosova, "Debunking Myths about Electronic Voting: Lessons from Twenty Years of E-Voting in Estonia," *Government Information Quarterly*, 38, 4, 2021.

[2]. S. Lee, L. Figueroa, B. Sun, R. Lin, "A blockchain-based e-voting system," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, 1013-1021, 2016.

[3]. Y. Liu, Q. Wang, "An e-voting protocol based on blockchain," *IACR Cryptology ePrint Archive*, Report 2017/1043, 2017.

[4]. N. Kshetri, J. Voas, "Blockchain-Enabled E-Voting," *IEEE Software*, 35, 4, 95-99, 2018.

[5]. Stevena, Fortino Hogan Hadiprodjoa, Islam Nur Alama, Lili Ayu Wulandharia, "Implementation of Blockchain-based Electronic Voting System: A Case Study in Indonesia," *Procedia Computer Science,* 269, 1-12, 2025.

[6]. M. V. Vladucu, "E-voting meets blockchain: A survey," *IEEE Access*, 11, 24874-24896, 2023.

[7]. Haber S., Stornetta W.S., "How to time-stamp a digital document," *J. Cryptol*, 3, 99-111, 1991.

[8]. P. McCorry, S. F. Shahandashti, F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Financial Cryptography and Data Security (FC)*, 357-375, 2017.

[9]. L. Xu, C. Chen, Y. Liu, Y. Wang, "A multi-candidate voting model based on blockchain," *IEEE/CAA Journal of Automatica Sinica*, 8, 12, 1858-1870, 2021.