Blockchain Enabled Voting System for Improving Election Transparency and Trust

Nasib Nasib[1], Aldila Dinanti[2], Fina Nailatul Izzah[3*], Az Zahrawani Ramadhan[4], Ikyboy Van Versie[5]
[1]Faculty of Economics, Institut Bisnis Informasi Teknologi dan Bisnis, Indonesia
[2]Faculty of Economics and Business, Universitas Jenderal Soedirman, Indonesia
[3,4]Faculty of Science and Technology, Universitas Raharja, Indonesia
[5]Department of Computer Science, Eesp Incorporation, Samudra Hindia Britania
[1]nasibwibowo02@gmail.com, [2]aldila.dinanti@unsoed.ac.id, [3]finanailatul@raharja.info, [4]azzahrawani@raharja.info, [5]vanrizkyid@eesp.io
***Corresponding Author**

Article Info

Article history:

Submission, 24-12-2025
Revised, 18-02-2026
Accepted, 05-05-2026
Published, 30-05-2026

Keywords:

Blockchain
Voting
Transparency
Trust
Security

ABSTRACT

Elections are a fundamental component of democratic systems, yet conventional paper based and centralized electronic voting mechanisms continue to face persistent challenges related to transparency, security, auditability, and declining public trust. To address these issues, **this study aims** to design and evaluate a blockchain enabled voting system that can improve election transparency and strengthen voter trust by leveraging decentralization, immutability, and cryptographic security. The research adopts a **system design and evaluation methodology** that integrates an in depth literature review, blockchain architecture modeling, smart contract development, and experimental evaluation focusing on security, transparency, and performance under simulated election conditions. **The results show** that the proposed system successfully ensures immutable vote recording, prevents double voting through automated smart contract enforcement, enhances end to end auditability via a transparent distributed ledger, and significantly improves resistance to vote manipulation and unauthorized access when compared to conventional and centralized electronic voting systems. Performance analysis indicates that while transaction latency increases with higher voting loads due to consensus mechanisms, the system remains stable, reliable, and operational, demonstrating feasibility for small to medium scale elections. Furthermore, the decentralized architecture reduces single points of failure and minimizes reliance on trusted third parties. **Overall**, this study concludes that blockchain technology provides a robust and trustworthy foundation for modern digital voting systems, while also highlighting scalability, computational overhead, and real world implementation challenges that should be addressed through optimization techniques and pilot deployments in future research.

This is an open access article under the CC BY 4.0 license.

DOI: https://doi.org/10.34306/bfront.v6i1.1035
This is an open-access article under the CC-BY license (https://creativecommons.org/licenses/by/4.0/
©Authors retain all copyrights

1. INTRODUCTION

Elections are a key pillar of democratic governance, allowing citizens to exercise political rights and legitimize public authority. Their credibility depends on transparency, integrity, fairness, and public trust, as confidence in accurate vote recording and counting strengthens democratic stability [1]. However, traditional voting systems, especially paper-based and centralized infrastructures, remain vulnerable to manipulation, miscounting, ballot loss, and delays in result reporting [2]. Centralized control over voter databases and vote-counting processes also creates single points of failure that may be exploited by insiders or cyber attackers, potentially weakening election integrity and public confidence [3]. As electoral systems grow more complex, maintaining transparency and accountability has become a major challenge for governments and election authorities [4, 5]. Electronic voting systems have been introduced to improve efficiency and accessibility [6], yet centralized e-voting platforms still raise concerns regarding security, privacy, transparency, and verifiability [7]. Their reliance on proprietary software and centralized servers often prevents independent verification, requiring stakeholders to trust election authorities and technology providers [8]. Studies also report vulnerabilities such as software errors, misconfigurations, malware attacks, and data breaches [9]. In addition, balancing voter anonymity with vote integrity remains difficult, as weak privacy protections may enable coercion while insufficient safeguards allow manipulation [10]. These challenges show that simple digitization is insufficient to ensure trustworthy elections, highlighting the need for technologies that embed transparency and accountability directly into electoral systems [11].

Blockchain technology offers a decentralized voting framework that enhances transparency, integrity, traceability, and protection against data manipulation through cryptographic security, timestamps, and immutable records [12, 13, 14]. Theoretically, blockchain supports distributed ledger governance and institutional governance by promoting decentralized consensus, accountability, and verifiable records to strengthen public trust [15, 16, 17]. In voting systems, votes can be recorded as verifiable transactions while preserving voter anonymity through digital signatures, hashing, privacy-preserving protocols, and smart contracts that automate election procedures and reduce human error [18, 19, 20]. Therefore, this study proposes a blockchain-enabled voting architecture that integrates decentralized vote recording, secure voter authentication, and verifiable vote tallying to improve transparency, security, scalability, and feasibility for real-world elections [21, 22].

This research supports SDGs 16 (Peace, Justice, and Strong Institutions), which emphasizes transparent and accountable democratic systems. By utilizing blockchain technology, the proposed voting system enhances electoral transparency, accountability, and auditability through decentralized and immutable records, reducing the risk of fraud and corruption. Positioned within the field of blockchain governance and Distributed Ledger Technologies (DLT), the system leverages decentralized consensus and cryptographic verification to strengthen institutional transparency. Through performance and scalability evaluation, this study also explores the optimization of blockchain infrastructure for governance applications, contributing to digital governance, institutional legitimacy, and increased citizen participation.

The research is guided by the following question: how a blockchain-enabled voting system can be designed and evaluated to improve transparency, trust, and security in elections while remaining scalable and feasible for real-world implementation. This question also explores the key factors influencing system adoption, including usability, regulatory considerations, and technological readiness, as well as how such a system can address existing challenges in conventional voting processes, such as fraud, lack of transparency, and limited public trust. Furthermore, the study aims to assess the system's performance and reliability through appropriate evaluation methods to ensure its effectiveness in practical, real-world election scenarios.

2. LITERATURE REVIEW

2.1. Blockchain Technology for Secure and Transparent Voting Systems

Blockchain technology has been widely studied as a foundational infrastructure for building secure and transparent digital systems due to its decentralized and immutable nature [23]. Recent studies emphasize that blockchain eliminates reliance on centralized authorities by distributing data storage and verification across multiple nodes, thereby reducing single points of failure and increasing system resilience [24]. In the context of voting systems, blockchain has been recognized as a promising solution to ensure transparency and integrity in electoral processes. Researchers argue that blockchain-based voting enables end-to-end verifiability, allowing stakeholders to independently verify that votes are correctly recorded and counted without revealing voter identities [25].

Recent studies show that blockchain's immutability plays an important role in preventing vote tampering and unauthorized changes to election data [26]. Once recorded on the blockchain, votes become extremely difficult to alter, which strengthens trust in election outcomes [27]. Blockchain networks also provide transparent audit trails that can be accessed by auditors and observers, increasing accountability and reducing disputes over election results [28]. Beyond elections, blockchain has been widely explored as an infrastructure for digital governance and public sector transparency, including applications in public records, digital identity, service delivery, and anti-corruption initiatives [29, 30]. Its decentralized and immutable characteristics enable verifiable and tamper-resistant records that improve accountability in governmental processes [31]. By situating blockchain-based voting within this broader governance context, this study aligns electoral innovation with ongoing digital governance transformation and presents a conceptual model illustrating how blockchain supports secure and transparent voting through decentralized vote submission, verification, and recording in a distributed ledger environment [32, 33].

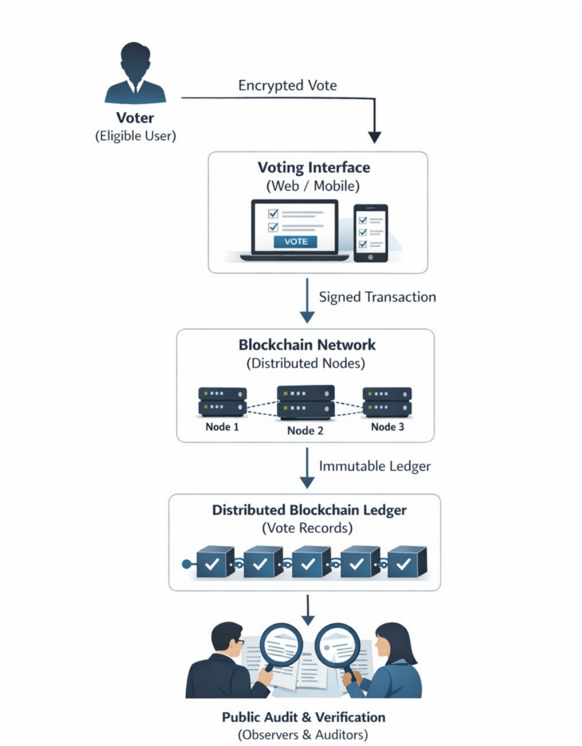

Figure 1. Conceptual Illustration of a Blockchain Based Voting System

Figure 1 illustrates a blockchain-based voting system in which votes are submitted as encrypted and digitally signed transactions. Each vote is verified by multiple distributed nodes before being permanently recorded in an immutable blockchain ledger. This decentralized verification process prevents vote tampering and unauthorized data modification. In addition, the transparent and auditable ledger allows independent verification of election results without revealing voter identities. Overall, the figure highlights how blockchain technology enhances transparency, integrity, and trust in electoral systems.

2.2. Security and Privacy Mechanisms in Blockchain-Based Voting

Recent literature emphasizes that while blockchain enhances transparency, it must be carefully integrated with cryptographic mechanisms to protect voter anonymity and prevent coercion [34]. Studies conducted after 2022 highlight the use of digital signatures, cryptographic hashing, and zero-knowledge proof techniques to ensure that votes remain confidential while still being verifiable [35]. Furthermore, researchers note that voter authentication is a key challenge in blockchain-based voting systems. Secure identity verification mechanisms must guarantee that only eligible voters can participate, while preventing double voting and identity fraud [36]. Several recent approaches combine blockchain with decentralized identity frameworks to achieve secure and privacy-preserving voter registration and authentication [37]. These solutions demonstrate that blockchain-based voting systems can achieve a balance between transparency and privacy when appropriate cryptographic protocols are applied, reinforcing voter trust without exposing sensitive personal information.

2.3. Smart Contracts and Automation in Voting Processes

Smart contracts have become a central component in modern blockchain-based voting architectures. Defined as self-executing programs deployed on blockchain platforms, smart contracts enable the automation of election rules and procedures [38]. Recent studies suggest that smart contracts can significantly reduce human intervention in voting processes, thereby minimizing administrative errors and opportunities for manipulation [39]. Election phases such as voter registration validation, vote casting, and result tallying can be encoded into smart contracts, ensuring consistent and transparent execution of predefined rules [40]. Post-2022 research also highlights the role of smart contracts in improving system reliability and auditability. Because smart contracts are publicly accessible and immutable once deployed, stakeholders can review and verify election logic before voting begins [41]. This transparency increases confidence in the correctness of election procedures and outcomes. However, recent literature also emphasizes the importance of formal verification and rigorous testing of smart contracts to prevent vulnerabilities that could compromise election integrity. These findings underline the necessity of secure smart contract design as a core element of blockchain-enabled voting systems [42].

2.4. Blockchain Applications for Enhancing Election Transparency and Trust

The application of blockchain technology in electoral systems has gained increasing attention as a way to improve transparency and public trust [43]. Empirical studies show that blockchain-based voting systems can enhance voter confidence by enabling transparent, auditable, and tamper-resistant election processes [44]. Transparency is supported through open access to transaction records, while trust is strengthened through cryptographic mechanisms that protect vote integrity and authenticity [45]. Research on digital trust further explains that trust in digital systems emerges from a combination of technological reliability, procedural fairness, and institutional legitimacy [46]. In both information systems and public administration research, transparency must be supported by governance structures and accountability mechanisms to effectively build public trust [47]. Therefore, blockchain-enabled voting can be understood not only as a decentralized technical solution but also as a governance-oriented digital trust system.

Recent studies also highlight the broader societal and institutional impacts of blockchain-based voting systems. Transparent digital voting infrastructures may increase voter participation and reduce skepticism toward electoral authorities, especially in environments with low institutional trust [48]. However, the literature also identifies challenges related to scalability, usability, and regulatory acceptance, indicating that successful implementation requires careful system design and policy alignment. From an interdisciplinary perspective, transparency and trust are shaped not only by technology but also by institutional and governance factors [49]. Transparency theory further suggests that accessible and verifiable digital processes can reduce information asymmetry and strengthen public confidence in governing institutions. Building on these perspectives, this study proposes a blockchain-enabled voting system that emphasizes transparency and trust while addressing security, performance, and practical feasibility considerations [50].

Blockchain technology also aligns with global governance initiatives such as the United Nations Sustainable Development Goals (SDGs), especially SDGs 16: Peace, Justice, and Strong Institutions, which emphasizes the importance of transparent, accountable, and inclusive institutions. In the context of electoral systems, transparent and verifiable voting infrastructures contribute to strengthening democratic governance, reducing the risk of electoral manipulation, and increasing public confidence in political institutions. Therefore, the integration of blockchain technology into voting systems not only addresses technical challenges related to security and transparency but also supports broader global efforts to improve institutional accountability and democratic participation.

3. RESEARCH METHOD

3.1. Research Design and Approach

This study adopts a system design and evaluation research approach, which is commonly used in blockchain and information systems research. The primary objective of this approach is to design, implement, and evaluate a blockchain-enabled voting system that enhances election transparency and public trust. The research focuses on both technical development and analytical evaluation, ensuring that the proposed system is not only theoretically sound but also practically feasible.

The research methodology integrates qualitative analysis through literature review and system modeling, as well as quantitative evaluation through performance and security assessment. This combined approach allows the study to analyze how blockchain characteristics such as decentralization, immutability, and transparency can address key challenges in conventional and electronic voting systems.

3.2. Research Stages

The research is conducted through a structured sequence of stages, starting from problem identification to system evaluation. Each stage is designed to ensure systematic development and validation of the proposed blockchain-based voting system.

To clearly describe the systematic process adopted in this study, summarizes the main research stages and their corresponding activities, outlining the methodological flow used to design, implement, and evaluate the proposed blockchain-based voting system.

Table 1. Research Stages and Activities

Research Stages	Description
Problem Identification	Identifying transparency, trust, and security issues in existing voting systems
Literature Review	Reviewing recent studies on blockchain, e-voting, smart contracts, and election security
System Requirement Analysis	Defining functional and non-functional requirements of the voting system
System Design	Designing the blockchain-based voting architecture and smart contracts
System Implementation	Developing and configuring the proposed voting system
System Evaluation	Evaluating transparency, security, and performance of the system
Result Analysis	Analyzing findings and identifying strengths and limitations

Table 1 presents a structured overview of the research methodology, starting from problem identification and literature review to system design, implementation, and evaluation. The staged approach ensures that the proposed voting system is developed based on clearly defined requirements and validated through systematic analysis. By following these research stages, the study maintains methodological rigor while enabling a comprehensive evaluation of how blockchain technology can enhance election transparency and trust.

3.3. Proposed Blockchain-Based Voting System Architecture

The proposed voting system is built on a decentralized blockchain architecture in which votes are recorded as immutable transactions within a distributed ledger. By removing reliance on a centralized authority, the system improves transparency, security, and reliability, since all transactions are validated and stored collectively by multiple network nodes. The system consists of several core components that support the voting process, including voter registration, voter authentication, vote casting, smart contract execution, and blockchain ledger storage. During the registration stage, eligible voters are verified and enrolled in the system according to predefined electoral requirements. Once registered, voters must complete a secure authentication process before accessing the voting interface, ensuring that only authorized participants are able to vote while maintaining voter confidentiality.

After successful authentication, voters can cast their votes through a secure digital voting interface. Each vote is encrypted and digitally signed before being transmitted to the blockchain network to guarantee confidentiality, authenticity, and data integrity. Smart contracts automatically implement election regulations, including preventing duplicate voting and ensuring that votes are submitted within the authorized voting period. Once validated by the network, the vote transaction is permanently stored in the blockchain ledger, where it becomes tamper-resistant and transparently verifiable. Because the ledger is distributed across multiple nodes, the recorded votes can be independently audited by authorized parties, enabling transparent election results and strengthening public trust in the electoral process.

3.4. Research Methodology Workflow

To illustrate the overall research methodology and system development process adopted in this study, the workflow of the proposed research, highlighting the sequential stages involved in designing, implementing, and evaluating the blockchain-based voting system.

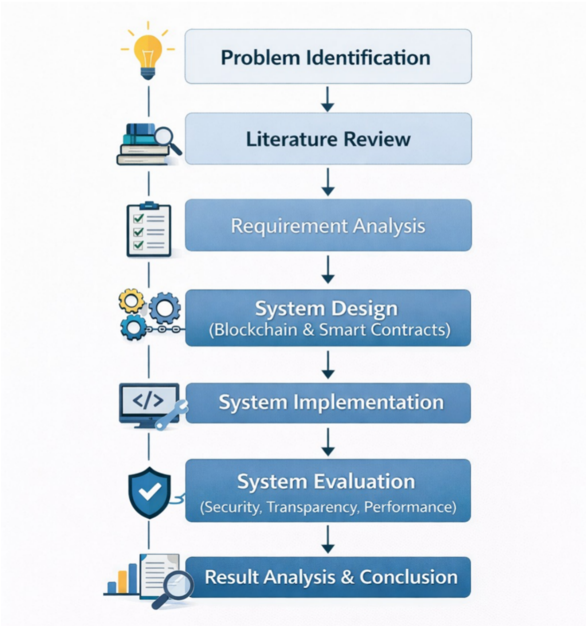

Figure 2. Workflow of the Research Methodology for Developing a Blockchain Based Voting System

Figure 2 depicts a structured research workflow that begins with problem identification and a comprehensive literature review to establish the theoretical foundation of the study. The process continues with system requirement analysis, which defines the functional and non-functional needs of the voting system, followed by system design incorporating blockchain technology and smart contracts. The designed system is then implemented and evaluated based on security, transparency, and performance criteria. Finally, the results of the evaluation are analyzed to assess the effectiveness of the proposed approach and to draw conclusions regarding its potential application in real-world electoral environments.

3.5. Data Collection and Analysis Techniques

This study uses secondary data and system-generated experimental data to evaluate the proposed blockchain-enabled voting system. Secondary data are obtained from recent academic literature, technical reports, and standards on blockchain and electronic voting to support system requirements and evaluation criteria. Primary data are collected through system experiments and simulations, including blockchain transaction records, block confirmation times, validation logs, and smart contract outputs. The evaluation focuses on transaction latency, throughput, confirmation time, and validation logs, as these metrics reflect voter responsiveness, system capacity during peak voting, vote finalization speed, and auditability. Therefore, the simulation provides practical insights into the system's operational performance and feasibility for real-world electoral implementation.

Data analysis is conducted using qualitative and quantitative approaches. Qualitative analysis evaluates transparency, auditability, and compliance with election requirements, while quantitative analysis measures performance indicators such as latency, throughput, and confirmation time. A comparative analysis with conventional and centralized electronic voting systems is also performed to assess improvements in transparency, security, and trust.

3.6. System Evaluation

The evaluation of the proposed system is conducted by analyzing its ability to address key election challenges. Security evaluation examines resistance to vote tampering and unauthorized access, while transparency evaluation focuses on auditability and verifiability of election data. Performance evaluation considers transaction processing efficiency and system scalability. The results of this evaluation are used to determine the feasibility of implementing blockchain-based voting systems in real-world electoral environments and to identify areas for future improvement.

4. RESULTS AND DISCUSSION

4.1. System Implementation Results

The blockchain-enabled voting system proposed in this study was successfully implemented based on the design specifications and methodological framework described in Chapter 3. The system integrates a decentralized blockchain network, smart contracts, and cryptographic mechanisms to support secure voter authentication, vote casting, and vote storage. Each vote submitted by a registered voter is encrypted, digitally signed, and stored as an immutable transaction on the blockchain ledger. The implementation confirms that smart contracts effectively enforce election rules, including voter eligibility verification, prevention of double voting, and enforcement of voting time constraints. While prior blockchain-based voting studies have primarily focused on conceptual frameworks or isolated security features, the originality of the proposed system lies in its integrated architectural design that operationalizes governance principles through enforceable smart contract mechanisms. Unlike approaches that merely record votes on-chain, this system embeds rule validation, voter eligibility checks, time-bound constraints, and duplicate vote prevention directly within the smart contract logic, ensuring automated procedural compliance. Furthermore, the architecture combines decentralized ledger storage with structured performance evaluation under simulated voting loads, enabling a comprehensive assessment of both governance integrity and operational feasibility. This integrated system-level approach distinguishes the present study from earlier works that emphasize conceptual blockchain adoption without detailed architectural enforcement mechanisms. Once a vote is recorded, it becomes permanently stored and cannot be altered or removed, ensuring data immutability.

4.2. Functional Validation of the Voting Process

Functional validation was conducted to assess whether each stage of the voting process operates correctly. The voter registration and authentication modules successfully verified voter eligibility before allowing access to the voting interface. Unauthorized users were prevented from submitting votes, ensuring compliance with election rules. During the vote casting phase, the system correctly recorded each vote as a unique blockchain transaction. The validation mechanism ensured that each voter could cast only one vote, and any attempt at duplicate voting was automatically rejected by the smart contract. These results confirm that the system provides reliable and consistent voting functionality, addressing common weaknesses in conventional and centralized electronic voting systems.

4.3. Transparency and Auditability Evaluation

Transparency and auditability are critical factors in building trust in electoral systems. The results show that the proposed blockchain-based voting system enables end-to-end transparency by maintaining a publicly verifiable ledger of voting transactions. Authorized election observers and auditors can independently verify the number of votes recorded and ensure that all votes are included in the final tally.

The immutable nature of the blockchain ensures that any attempt to manipulate vote data would be immediately detectable. Unlike traditional voting systems that rely on centralized authorities, the proposed system distributes trust across multiple nodes, significantly reducing the potential for manipulation or biased control. These findings demonstrate that blockchain technology effectively enhances transparency and accountability in the electoral process. In practical terms, enhanced auditability enables election observers, regulatory bodies, and independent auditors to verify vote inclusion and integrity without relying solely on centralized authorities. This reduces post-election disputes and strengthens institutional legitimacy. For public sector practitioners, such audit mechanisms can also serve as a model for other governance processes requiring verifiable digital records.

4.4. Security and Integrity Assessment

Security analysis indicates that the proposed system provides strong protection against vote tampering, unauthorized access, and data manipulation. Cryptographic techniques, including hashing and digital signatures, ensure that each vote is authentic and verifiable. Any modification to stored voting data would result in hash mismatches, making tampering attempts easily detectable. Additionally, the decentralized blockchain architecture minimizes the risk of single points of failure and insider threats, which are common vulnerabilities in centralized voting infrastructures.

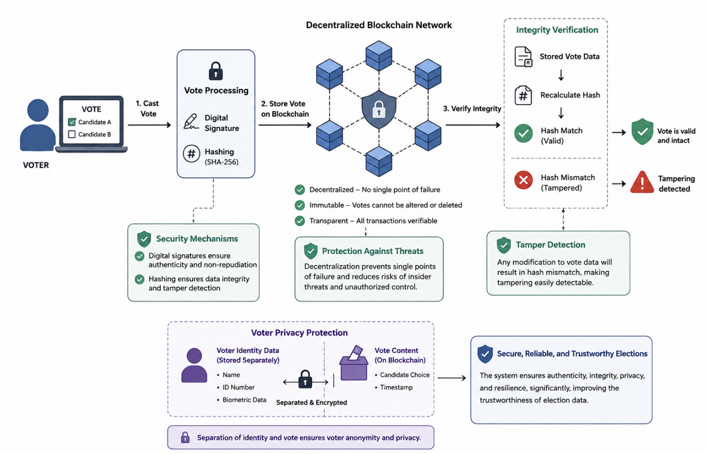

Figure 3. Security and Integrity Features of the Blockchain Based Electronic Voting System

Figure 3 illustrates the security and integrity mechanism of the proposed blockchain-based electronic voting system. As shown in the figure, the voting process begins with voter authentication, followed by vote encryption, digital signature validation, and hash generation before the vote is stored in a decentralized blockchain network. The figure also highlights key security functions, including tamper detection through hash mismatch alerts, unauthorized access prevention, and voter privacy protection by separating voter identity from vote content. These mechanisms demonstrate that the proposed system can enhance vote authenticity, verifiability, immutability, privacy, and resilience against single points of failure.

4.5. Performance and Scalability Results

Performance evaluation using experimental data shows that the proposed blockchain-based voting system can process transactions within acceptable time limits under simulated voting loads. Compared with public blockchains and centralized e-voting systems, this architecture offers moderate latency while improving transparency, tamper resistance, and system reliability. Although latency increases with voter volume due to consensus mechanisms, the system remains stable without data loss, making it feasible for small to medium-scale elections. For large-scale national use, further optimization through permissioned blockchain, layer-2 scaling, or hybrid on-chain/off-chain models is required to improve throughput and scalability.

4.6. Comparative Analysis with Conventional Voting Systems

A comparative evaluation of the proposed blockchain-based voting system and conventional methods, including paper-based and centralized electronic voting systems, shows that the blockchain approach offers greater transparency, auditability, and data integrity. Unlike many previous studies that focus mainly on cryptographic security or theoretical decentralization, this framework integrates governance aspects by aligning smart contract mechanisms with institutional election rules. The study also strengthens existing research by incorporating scalability testing, performance evaluation, and feasibility analysis under different voting loads, providing empirical validation often absent in earlier models. Compared with traditional election systems, the proposed approach eliminates reliance on trusted third parties through decentralized consensus, although it introduces higher technical complexity and computational demands. Paper-based elections rely heavily on manual procedures that are prone to human error and logistical inefficiencies, while centralized electronic systems improve efficiency but still face transparency limitations and single points of failure. In contrast, blockchain-based voting provides verifiable and tamper-resistant records, highlighting a trade-off between operational simplicity and governance-level transparency and emphasizing the need for balanced and context-aware adoption strategies in real-world electoral systems.

4.7. Discussion of Research Objectives and Findings

The results of this study show that the proposed blockchain-enabled voting system effectively improves election transparency, security, and public trust through immutable and auditable vote records while reducing reliance on centralized control. In addition to electoral applications, the findings highlight the broader potential of blockchain technology in supporting public sector transparency, such as in budget monitoring, public procurement, digital identity management, and policy auditing, by enabling verifiable public records and strengthening accountability in digital governance. However, the study also identifies limitations related to scalability, system complexity, and implementation costs. To address these challenges, several practical strategies are recommended, including phased pilot implementations, the use of permissioned blockchain architectures to manage computational demands, and hybrid models that combine on-chain verification with off-chain processing. Strong governance frameworks, including cybersecurity management and regulatory alignment, are also necessary to ensure sustainable operation. Although further research and real-world testing are still required, the findings indicate that blockchain technology has strong potential to enhance transparency and trust in modern electoral systems.

5. MANAGERIAL IMPLICATIONS

The findings of this study provide important implications for policymakers, election authorities, and technology decision-makers considering blockchain-based voting systems. The improved transparency and auditability suggest that election management bodies should consider decentralized architectures to reduce single points of failure and increase public trust in election results. The use of smart contracts also indicates that governance processes such as voter verification, voting procedures, and vote counting can be automated, helping reduce human error, administrative bias, and operational inefficiencies while shifting managerial roles toward system monitoring and compliance oversight.

In addition, the performance and scalability results highlight the need for careful planning in technology implementation. Decision-makers should evaluate election scale, network capacity, and computational resources before adopting blockchain systems. For large-scale elections, approaches such as permissioned blockchains or layer-2 solutions may help balance security and efficiency. A gradual integration strategy such as initially using blockchain for vote auditing, result verification, or post-election transparency can support smoother adoption. Furthermore, investment in cryptographic infrastructure, technical expertise, staff training, and cybersecurity governance is necessary to ensure reliable system operation, regulatory compliance, and long-term public trust in digital electoral technologies.

6. CONCLUSION

This study concludes that the proposed blockchain-enabled voting system is effective in enhancing election transparency, security, and public trust. The results demonstrate that the integration of decentralized blockchain architecture and smart contracts enables immutable vote recording, transparent audit trails, and secure enforcement of election rules. The system successfully addresses key weaknesses of conventional and centralized electronic voting systems, particularly in terms of data integrity, auditability, and resistance to manipulation. Overall, the findings confirm that blockchain technology provides a robust and reliable foundation for modern digital voting systems.

The research questions of this study are adequately answered through system implementation and evaluation. The findings indicate that blockchain-based voting can significantly improve transparency and trust by eliminating single points of failure and enabling independent verification of election results. However, this study also has several limitations. The system evaluation was conducted under simulated conditions, and real-world electoral complexities such as large-scale voter participation, legal constraints, and infrastructure readiness were not fully addressed. In addition, scalability and computational overhead remain significant challenges for the adoption of blockchain in nationwide elections.

Future research should focus on improving the scalability and performance of blockchain-based voting systems to better support large-scale electoral processes. Further studies may explore hybrid architectures, permissioned blockchains, or layer-2 solutions to reduce latency and computational costs. Moreover, future research should involve real-world pilot implementations and take into account legal, social, and regulatory factors to ensure practical feasibility. By addressing these aspects, future studies can contribute to the development of secure, transparent, and trustworthy electoral systems suitable for broader adoption.

7. DECLARATIONS

7.1. About Authors

Nasib Nasib (NN) https://orcid.org/0000-0003-3798-1562
Aldila Dinanti (AD) https://orcid.org/0000-0002-7009-8045
Fina Nailatul Izzah (FN) https://orcid.org/0009-0008-5974-9944
Az Zahrawani Ramadhan (AZ) https://orcid.org/0009-0009-6915-0000
Ikyboy Van Versie (IV) https://orcid.org/0009-0004-0232-6044

7.2. Author Contributions

Conceptualization: NN, AD, and FN; Methodology: AZ; Software: IV; Validation: NN and AD; Formal Analysis: FN and AZ; Investigation: IV; Resources: FN; Data Curation: AD; Writing Original Draft Preparation: AZ and NN; Writing Review and Editing: IV; Visualization: AD; All authors, NN, AD, FN, AZ and IV, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

[1] 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, 2024.
[2] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," *IEEE Access*, vol. 10, pp. 59 959–59 969, 2022.
[3] S. Pandya, "Advanced blockchain-based framework for enhancing security, transparency, and integrity in decentralised voting system," *Int. J. Adv. Res. Sci. Commun. Technol*, vol. 2, no. 1, pp. 865–876, 2022.
[4] S. Shuker and N. Hussain, "Building secure e-voting systems: A blockchain approach for transparent democracy," *Unpublished Manuscript*, 2024.
[5] J. M. Simatupang and E. Indrayani, "Blockchain adoption readiness: Expert perspectives on policy, implementation, and governance in indonesia," *Jurnal Bina Praja*, 2025. [Online]. Available: https://jurnal.kemendagri.go.id/index.php/jbp/article/view/2681
[6] I. Singh, A. Kaur, P. Agarwal, and S. M. Idrees, "Enhancing security and transparency in online voting through blockchain decentralization," *SN Computer Science*, vol. 5, no. 7, p. 921, 2024.
[7] 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, 2023.
[8] Z. Haider and M. Daniel, "Blockchain technology for enhanced security and trust in e-voting systems," 2024.
[9] A. Z. Abbasi, S. Bashir, M. Albashrawi, and D. H. Ting, "Blockchain enabled e-voting system adoption: examining the mediating role of perceived transparency," *Journal of Asia Business Studies*, vol. 19, no. 3, pp. 660–683, 2025.
[10] A. Gunawan, M. M. Siahaan, R. Adyatama, T. Kerimbekov, and K. Vaher, "Distributed data integrity and decentralized storage leveraging ipfs in blockchain systems," *Blockchain Frontier Technology*, vol. 5, no. 2, pp. 158–171, 2026.
[11] V. Ghosh and H. Gupta, "A blockchain-based e-voting system for secure and transparent elections," in *International Conference on ICT for Sustainable Development*. Springer, 2024, pp. 163–173.

[12] A. Shaikh, N. Adhikari, A. Nazir, A. S. Shah, S. Baig, and H. Al Shihi, "Blockchain-enhanced electoral integrity: a robust model for secure digital voting systems in oman," *F1000Research*, vol. 14, p. 223, 2025.

[13] O. O. Olaniyi, "Ballots and padlocks: Building digital trust and security in democracy through information governance strategies and blockchain technologies," *Available at SSRN 4759942*, 2024.

[14] N. Khairunnisa, F. Christiani, and A. G. Prawiyogi, "Supply chain transparency: Exploring blockchain solutions for enhanced traceability and efficiency," *Blockchain Frontier Technology*, vol. 4, no. 1, pp. 15–22, 2024.

[15] S. Reddaiah, R. Subramanyam, J. Refonaa, S. J. Shabu, S. Praveen *et al.*, "Blockchain-enabled decentralized trust management and secure voting system," in *2024 4th International Conference on Pervasive Computing and Social Networking (ICPCSN)*. IEEE, 2024, pp. 554–559.

[16] D. D. Bhavani, R. Gayathri, M. Bhagavanthu, A. Sheeba, M. Sampoornam, and P. Bhuvaneshwari, "Blockchain-based voting systems enhancing transparency and security in electoral processes," in *ITM Web of Conferences*, vol. 76. EDP Sciences, 2025, p. 02004.

[17] L. Sahasra, T. A. Reddy, and K. V. Sharma, "Empowering voting integrity: An empirical study of blockchain smart contracts in electoral systems," *International Journal of Computer Engineering in Research Trends*, vol. 10, no. 11, pp. 37–46, 2023.

[18] S. Revathi and V. ELangovan, "Fostering democratic transparency: A secure voting system with aadhaar cards on the ethereum blockchain technology," in *International Conference on Mathematical Modeling and Computational Science*. Springer, 2025, pp. 477–498.

[19] R. Minu and G. Nagarajan, "Blockchain-enabled decentralized trust management and secure voting system," in *2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT)*, vol. 1. IEEE, 2024, pp. 21–26.

[20] V. V. Febiandini and M. S. Sony, "Analysis of public administration challenges in the development of artificial intelligence industry 4.0," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 4, no. 2, pp. 164–168, 2023.

[21] J. B. Hendrawidjaja, B. W. Soetjipto, R. D. Kusumastuti, and O. Jayanagara, "Ecosystem exchange, strategic capabilities, and firm performance with agility and innovation mediators," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 226–238, 2026.

[22] A. Tedyyana, O. Ghazali, T. Asnafi, O. W. Purbo, N. Z. Harun, and F. Riza, "Transforming the voting process integrating blockchain into e-voting for enhanced transparency and securiy," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 22, no. 2, pp. 311–320, 2024.

[23] 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 voting system," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 9, pp. 6855–6871, 2022.

[24] V. Agarwal, M. Lohani, A. S. Bist, and D. Julianingsih, "Application of voting based approach on deep learning algorithm for lung disease classification," in *2022 International Conference on Science and Technology (ICOSTECH)*. IEEE, 2022, pp. 01–07.

[25] F. Abo-Akleek, M. Mowafi, E. S. Taqieddin, and A. S. Shatnawi, "Leveraging blockchain for robust and transparent e-voting systems," *Cyber Security and Applications*, vol. 3, p. 100086, 2025.

[26] M. A. U. K. Atik, S. S. Tarin, M. Rahman, A. A. Alvi, and M. F. A. A. Sohan, "A comprehensive analysis of blockchain-based voting systems: Enhancing transparency and security," in *Proceedings of the 3rd International Conference on Computing Advancements*, 2024, pp. 733–740.

[27] H. O. Ohize, A. J. Onumanyi, B. U. Umar, L. A. Ajao, R. O. Isah, E. M. Dogo, B. K. Nuhu, O. M. Olaniyi, J. G. Ambafi, V. B. Sheidu *et al.*, "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges," *Cluster Computing*, vol. 28, no. 2, p. 132, 2025.

[28] I. P. Gustiah and H. Newell, "Enhancing human resource management efficiency through scalable blockchain networks with an adaptive ai approach," *Startupreneur Business Digital (SABDA Journal)*, vol. 4, no. 2, pp. 114–123, 2025.

[29] A. Nigmatov, A. Pradeep, and N. Musulmonova, "Blockchain technology in improving transparency and efficiency in government operations," in *2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2023, pp. 01–06.

[30] P. Kumbharkar, S. Pawtekar, S. Javeer, and P. Abhale, "Blockchain-based e-voting systems: Enhancing security transparency and trust," *International Journal of Science and Research Archive*, vol. 12, no. 1,

pp. 635–642, 2024.
[31] A. Sharma, D. Tirpathy *et al.*, "Electronic voting system using blockchain and machine learning," in *2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE)*. IEEE, 2024, pp. 1–7.
[32] A. Srivastava, P. Meshram, M. Negi, A. Narang *et al.*, "Blockchain-based voting systems: Integrity and trust in electoral events with secure ballot," in *Progressive Computational Intelligence, Information Technology and Networking*. CRC Press, pp. 608–614.
[33] A. R. Aruan, K. Toha, and A. R. Nurdin, "Digital governance for confiscating crypto-assets to settle tax liabilities in indonesia," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 7, no. 3, pp. 1066–1079, 2025.
[34] H. Peter, "Blockchain-based voting systems a secure and transparent future," *vol*, vol. 2, pp. 1–12, 2024.
[35] A. Feroz, D. Pranay, B. S. S. Raj, C. H. Vardhan, B. R. Raja, B. Nirmala, and P. Dharnasi, "Blockchain and machine learning combined secured voting system," *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, vol. 9, no. 1, pp. 119–124, 2026.
[36] L. L. Scientific, "The development of a blockchain-based system for electronic voting," *Journal of Theoretical and Applied Information Technology*, vol. 102, no. 17, 2024.
[37] M. Alown, M. S. Kiraz, and M. A. Bingol, "Enhancing democratic processes: A survey of dre, internet, and blockchain in electronic voting systems," *IEEE Access*, vol. 13, pp. 20 512–20 545, 2025.
[38] M. Sharma, A. Singh, and G. Varshney, "Enhancing electoral processes: The role of "smart voting systems"," in *Emerging Trends in Computer Science and Its Application*. CRC Press, 2025, pp. 501–505.
[39] V. Azhaguramyaa, J. Janet, M. Akilesh, M. Chandrasekaran, P. Dharaneesh, and K. Divvyananth, "Fusion of ai and blockchain for ensuring security and transparency in voting system," in *AIP Conference Proceedings*, vol. 3204, no. 1. AIP Publishing LLC, 2025, p. 020018.
[40] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, "Implementation of blockchain-based e-voting system," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 1449–1480, 2024.
[41] B. M. B. Pereira, J. M. Torres, P. M. Sobral, R. S. Moreira, C. P. d. A. Soares, and I. Pereira, "Blockchain-based electronic voting: A secure and transparent solution," *Cryptography*, vol. 7, no. 2, p. 27, 2023.
[42] M. H. R. Chakim, M. A. D. Yuda, R. Fahrudin, D. Apriliasari *et al.*, "Secure and transparent elections: Exploring decentralized electronic voting on p2p blockchain," *ADI Journal on Recent Innovation*, vol. 5, no. 1Sp, pp. 54–67, 2023.
[43] C. Anwar ul Hassan, M. Hammad, J. Iqbal, S. Hussain, S. S. Ullah, H. AlSalman, M. A. Mosleh, and M. Arif, "A liquid democracy enabled blockchain-based electronic voting system," *Scientific programming*, vol. 2022, no. 1, p. 1383007, 2022.
[44] V. Diaconita, A. Belciu, and M. G. Stoica, "Trustful blockchain-based framework for privacy enabling voting in a university," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 18, no. 1, pp. 150–169, 2023.
[45] M. K. Ahmed, R. D. Delmut, and M. Habila, "A review of blockchain-based e-voting systems: Enhancing security and transparency," *BIMA JOURNAL OF SCIENCE AND TECHNOLOGY GOMBE*, vol. 8, no. 3A, pp. 65–78, 2024.
[46] V. Poornachandran *et al.*, "Securing the vote: Leveraging anomaly detection in blockchain systems," *International Journal of Engineering Research and Sustainable Technologies (IJERST)*, vol. 2, no. 4, pp. 19–25, 2024.
[47] H. Misni, B. Jokonowoa, and H. Santoso, "Ensuring trust and integrity: a revolutionary approach to electronic voting through blockchain," *International Journal of Artificial Intelligence Research*, vol. 7, no. 2, 2024.
[48] U. Waheed, M. A. Khan, Y. Mansoor, H. Jamshed, and A. Hussain, "Blockchain-driven e-voting: Enhancing security and integrity with smart contracts," *Journal of Independent Studies and Research Computing*, vol. 23, no. 1, pp. 16–22, 2025.
[49] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of blockchain solutions for e-voting: a systematic literature review," *IEEE Access*, vol. 10, pp. 70 746–70 759, 2022.
[50] J. P. Neelammai, S. Keerthana, R. Aarthi, and S. B. Hamshika, "Blockchain-based online voting system using poa consensus," *Mathematics and Computational Sciences*, vol. 7, no. 1, pp. 34–44, 2026.