Jurnal Testing dan Implementasi Sistem Informasi
Vol 3(2) 2025 : 70-83

DESIGN AND IMPLEMENTATION OF A DECENTRALIZED E-VOTING SYSTEM ON LOCAL SERVER INFRASTRUCTURE

Tengku Mohd Diansyah[1*], Nuraminah Ramli[2], Muzammil Jusoh[3]
Faculty of Intelligent Computing Universiti Malaysia Perlis (UniMAP), Arau 02600, Malaysia[1,2]
Faculty of Electronic Engineering Technology, Universiti Malaysia Perlis (UniMAP), Arau 02600, Malaysia[3]
Universitas Harapan Medan, Sumatera Utara, Indonesia[1]
dian.10.22@gmail.com[1*], nuraminah@unimap.edu.my[2], muzammil@unimap.edu.my[3]

Received: 05 June 2025, Revised: 15 November 2025, Accepted: 01 December 2025
**Corresponding Author*

ABSTRACT
This study addresses the limitations of existing decentralized e-voting systems, particularly their reliance on public distributed infrastructures, limited real-world deployment feasibility, and lack of comprehensive evaluation. Previous studies have demonstrated the potential of distributed ledger-based voting mechanisms; however, most focus on conceptual designs or small-scale prototypes without detailed performance and usability validation. To address this gap, this research proposes and implements a decentralized e-voting system deployed on a local server infrastructure using distributed ledger technology and automated validation mechanisms for vote integrity. The system is designed to reduce dependency on external networks while maintaining transparency, immutability, and operational efficiency. The system was evaluated through functional testing, performance analysis, and user acceptance testing involving 30 participants in a controlled environment with 20 simulated voters. The results show that the system achieved a functional accuracy of 96% across 25 test scenarios. The average transaction response time ranged between 0.6 and 1.6 seconds, indicating efficient processing under moderate load conditions. However, the evaluation is limited to small-scale simulations and does not include stress testing, large-scale scalability analysis, or advanced security validation. Therefore, the findings demonstrate system feasibility rather than fully validated effectiveness. These results suggest that decentralized e-voting systems deployed on local infrastructures can provide a practical and efficient solution for controlled election environments, while further research is required to evaluate scalability, security robustness, and real-world deployment readiness.
Keywords : *Decentralized E-Voting, Distributed Ledger Technology, Smart Contract, Electronic Voting System, Blockchain-based Voting.*

1. Introduction

Electronic voting (e-voting) systems have emerged as a promising solution to improve the efficiency, accessibility, and transparency of electoral processes in both governmental and organizational contexts. Traditional voting systems, whether paper-based or electronically centralized, often suffer from several limitations, including high operational costs, limited scalability, susceptibility to fraud, and lack of transparency. Centralized e-voting systems, in particular, introduce critical risks such as single points of failure, vulnerability to insider attacks, and limited auditability, which collectively undermine public trust in election outcomes (Jafar et al., 2021; Vladucu et al., 2023).

To overcome these limitations, recent research has increasingly focused on leveraging blockchain technology and decentralized architectures for e-voting systems. Blockchain, as a form of distributed ledger technology (DLT), provides key properties such as immutability, transparency, and fault tolerance, which are highly desirable in electoral systems. In addition, smart contracts enable the automation of voting procedures, including voter authentication, vote casting, and tallying, thereby reducing human intervention and minimizing the risk of manipulation (Al-Madani et al., 2020; Patra et al., 2025). These features have positioned blockchain-based e-voting systems as a viable alternative to traditional centralized solutions.

Despite these advantages, the current body of research reveals several critical limitations and unresolved challenges. First, many existing blockchain-based e-voting systems primarily focus on conceptual frameworks or prototype implementations without comprehensive evaluation in real-world scenarios. For instance, studies such as Al-Madani et al. (2020) and Prasad et al. (2024) demonstrate the feasibility of smart contract-based voting mechanisms; however, their evaluations are often limited to basic functionality and do not sufficiently address scalability, usability, or deployment constraints. Similarly, Patra et al. (2025) emphasizes security and transparency through cryptographic mechanisms but provides limited empirical evidence regarding system performance under large-scale voting conditions.

Second, several studies highlight fundamental challenges related to voter privacy, coercion resistance, and anonymity. While blockchain ensures transparency and immutability, it may conflict with the requirement to preserve voter confidentiality. Ensuring that votes remain anonymous while still being verifiable is a complex problem that has not been fully resolved (Benabdallah et al., 2022; Berenjestanaki et al., 2023). Furthermore, coercion resistance—ensuring that voters cannot be forced to reveal or alter their votes—remains a significant challenge in digital voting environments (Almeida et al., 2023). These issues indicate that blockchain alone is not a complete solution and must be carefully integrated with cryptographic and system design strategies.

Third, most existing implementations rely heavily on public blockchain platforms such as Ethereum. While these platforms provide robust decentralization, they introduce several practical limitations, including high transaction costs (gas fees), network latency, scalability bottlenecks, and lack of control over infrastructure (Daraghmi et al., 2024; Ohize et al., 2025). These constraints make public blockchain solutions less suitable for localized or institutional voting scenarios, such as university elections or organizational decision-making processes, where cost efficiency, speed, and infrastructure control are critical requirements.

In addition, regulatory and operational considerations are often overlooked in existing studies. Real-world deployment of e-voting systems must comply with legal frameworks, data protection regulations, and organizational policies. However, many prior works focus primarily on technical design without addressing these broader implementation challenges (Kusi & Asoma, 2025). This gap highlights the need for practical and adaptable solutions that can be implemented in controlled environments while still maintaining essential security properties.

Based on these limitations, a clear research gap can be identified: the lack of decentralized e-voting systems that are not only secure and transparent but also practically deployable within controlled, local infrastructures. In particular, there is limited research on systems that combine distributed ledger technology and smart contracts within a local server environment to achieve a balance between decentralization, performance efficiency, and operational feasibility.

To address this gap, this study proposes and implements a decentralized e-voting system based on distributed ledger technology and smart contracts, deployed on a local server infrastructure. Unlike public blockchain-based approaches, the proposed system aims to reduce dependency on external networks while maintaining key properties such as data integrity, transparency, and fault tolerance. The use of smart contracts enables automated validation of voting processes, ensuring that election rules are enforced consistently and securely.

Furthermore, this study contributes by evaluating the proposed system through functional testing, performance analysis, and user acceptance testing, providing empirical evidence of its feasibility in a controlled environment. By focusing on practical deployment and system evaluation, this research aims to bridge the gap between conceptual blockchain-based voting models and real-world implementation requirements.

2. Literature Review

The development of electronic voting (e-voting) systems has evolved significantly with the adoption of distributed and decentralized technologies. This section critically reviews prior studies based on three main aspects: (1) architectural approaches to e-voting systems, (2) the role of distributed ledger and automated validation mechanisms, and (3) persistent challenges in security, privacy, and system deployment.

2.1 Centralized and Distributed E-Voting Architectures

Conventional e-voting systems are predominantly built on centralized architectures, where a single authority is responsible for managing voter registration, vote storage, and result computation. While such systems offer simplicity in implementation, they introduce critical risks, including lack of transparency, vulnerability to manipulation, and dependence on a single trusted entity (Khan et al., 2022; Gupta & Tyagi, 2025). These limitations reduce system reliability and public trust, particularly in high-stakes electoral environments.

In response, distributed approaches have been proposed to mitigate these issues. By distributing data across multiple nodes, decentralized systems improve fault tolerance, auditability, and resistance to tampering. Previous studies demonstrate that distributed voting architectures can enhance integrity by eliminating single points of failure and enabling independent verification of results (Hardwick et al., 2018; Jumaa & Shakir, 2023). However, these systems often introduce challenges related to coordination, synchronization, and system complexity.

2.2 Distributed Ledger and Automated Voting Mechanisms

Recent advancements in distributed ledger technology (DLT) have provided new opportunities for designing secure and transparent e-voting systems. DLT enables the storage of voting records in an immutable and append-only structure, ensuring that once a vote is recorded, it cannot be altered without detection. In addition, programmable validation mechanisms—commonly referred to as smart contracts—allow the automation of voting rules, including voter eligibility verification, vote casting procedures, and result aggregation (Tang et al., 2023).

Several studies have demonstrated the effectiveness of combining distributed ledgers with automated execution logic to enhance system transparency and reliability. For example, Spanos and Kantzavelou (2025) present a distributed voting system in which automated scripts enforce election rules and ensure data consistency across nodes. Similarly, Singh et al. (2023) propose a decentralized voting platform that leverages programmable validation to reduce human intervention and increase trust in the system.

Despite these advancements, many implementations remain limited to experimental or prototype stages. Furthermore, systems based on large-scale public distributed networks often face practical constraints, including processing delays, resource consumption, and limited control over system parameters. These issues can hinder their applicability in controlled environments where efficiency and predictability are essential (Fatih et al., 2023).

2.3 Security, Privacy, and Coercion Resistance

Security and privacy are fundamental requirements in e-voting systems. While distributed ledger technologies ensure data integrity and transparency, they do not inherently guarantee voter anonymity. In fact, the transparent nature of distributed records may conflict with the requirement to maintain ballot secrecy, creating a trade-off between verifiability and privacy (Ali, 2025).

One of the most challenging issues in this domain is achieving coercion resistance, which ensures that voters cannot be forced to disclose or alter their choices. Existing studies indicate that many distributed e-voting systems do not fully address this issue, particularly in remote voting scenarios where external influence cannot be easily controlled (Mookherji et al., 2022). Additionally, ensuring end-to-end verifiability while preserving anonymity remains an open research problem.

Another concern is the protection of voter identity and sensitive data. Although various cryptographic techniques have been proposed, their implementation is often inconsistent, and there is no universally accepted framework for secure and private distributed e-voting systems (Brasser, 2021). These limitations highlight the need for more robust and standardized approaches.

2.4 Scalability, Usability, and Deployment Considerations

In addition to security, practical factors such as scalability and usability significantly influence the adoption of e-voting systems. Large-scale elections require systems capable of handling high transaction volumes within strict time constraints. However, many distributed voting systems struggle to achieve the required level of performance, particularly when operating in resource-constrained environments (Marouan et al., 2025).

Usability is another critical factor that is often overlooked. E-voting systems must be accessible and user-friendly to ensure broad participation. Complex interfaces or technical barriers can reduce user trust and participation rates (Brasser, 2021). Despite its importance, usability evaluation is rarely conducted systematically in existing research.

Furthermore, most studies assume deployment on open and large-scale distributed networks, without considering alternative environments such as private or locally managed infrastructures. This assumption limits the applicability of existing solutions in scenarios where controlled environments are preferred, such as institutional or organizational elections.

2.5 Research Gap

Based on the above analysis, several research gaps can be identified:

1. Limited exploration of locally deployed distributed ledger systems compared to large-scale public infrastructures.
2. Lack of comprehensive evaluation, particularly in terms of scalability, usability, and real-world deployment.
3. Insufficient attention to privacy, coercion resistance, and regulatory considerations.
4. Absence of solutions that effectively balance decentralization and operational efficiency in controlled environments.

2.6 Research Positioning

To address these gaps, this study proposes a decentralized e-voting system that utilizes distributed ledger technology and automated validation mechanisms within a local server infrastructure. The proposed approach aims to provide a practical and efficient alternative to large-scale distributed systems by maintaining essential security properties while improving performance, usability, and deployment feasibility in controlled environments.

3.1 Research Methods

3.1 Research Approach

This study adopts the Design Science Research (DSR) methodology to develop and evaluate a decentralized e-voting system. DSR is chosen because it enables the systematic design, implementation, and evaluation of an artifact to solve real-world problems. The research process follows six main stages: problem identification, objective definition, system design, implementation, evaluation, and communication.

The primary objective is to design a secure, transparent, and efficient e-voting system that operates within a locally managed distributed environment, reducing dependency on external infrastructures while maintaining essential properties such as data integrity and auditability.

3.2 System Architecture Design

The proposed system is based on a distributed ledger architecture deployed on a local server infrastructure. The system consists of three main components:

1. Client Layer
   Provides user interfaces for voters and administrators, including voter registration, authentication, vote casting, and result visualization.
2. Application Layer
   Handles business logic, including voter validation, ballot management, and interaction with the distributed ledger.
3. Distributed Ledger Layer

Stores voting records in an immutable and append-only structure. Each transaction represents a vote that is validated and recorded across nodes.

To maintain controlled decentralization, the system uses a private distributed ledger configuration, where participating nodes are managed within a local network environment. This approach improves performance, reduces latency, and ensures better control over system operations compared to large-scale public infrastructures.

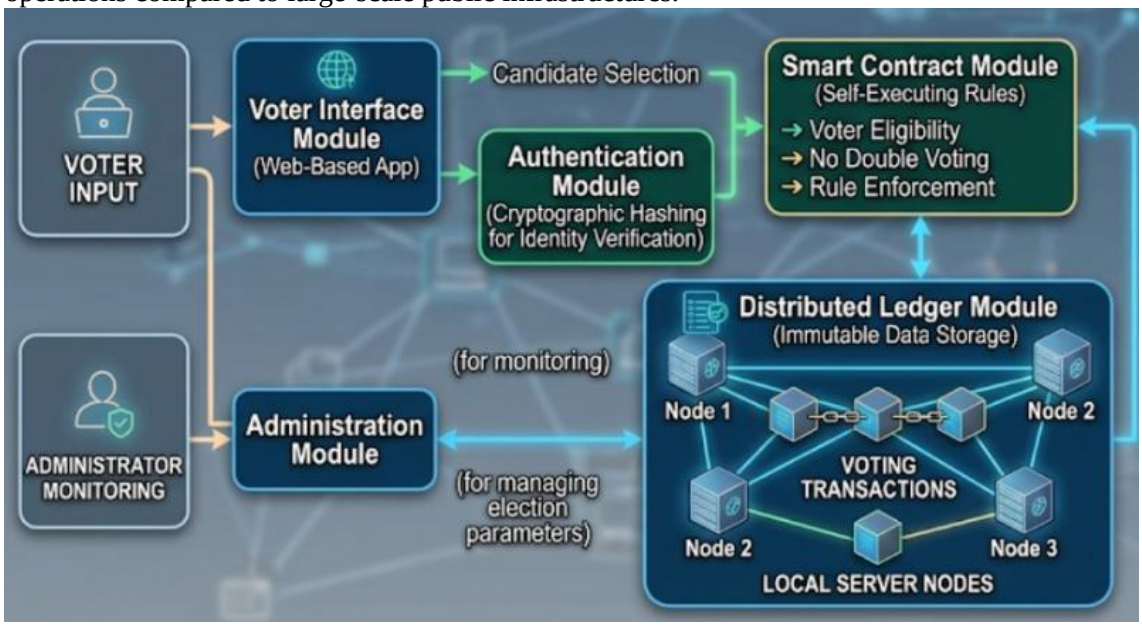

Figure 1. Architecture Design for E-voting Decentralized

Figure 1 illustrates the architecture of the proposed decentralized e-voting system deployed within a local distributed environment. The system is designed using a multi-layer architecture consisting of user interfaces, application logic, validation mechanisms, and a distributed ledger layer.

At the top layer, the system includes two primary interfaces: the voter interface and the administrator interface. The voter interface allows users to perform essential actions such as authentication and vote casting, while the administrator interface is responsible for managing election parameters, including voter registration and result monitoring. Both interfaces communicate directly with the central application server.

The application server acts as the core processing unit that handles incoming requests from users. It is responsible for coordinating system operations and forwarding voting transactions to the validation component. This layer ensures that all interactions between users and the system are properly managed and processed.

The validation logic component plays a critical role in enforcing election rules. It performs automated checks to ensure that only eligible voters can cast votes, prevents duplicate voting, and verifies the integrity of submitted data. This mechanism replaces manual validation processes, thereby increasing system reliability and reducing the risk of human error.

Once validated, voting transactions are forwarded to the distributed ledger layer, where all votes are recorded in an immutable and append-only structure. The ledger is maintained across multiple nodes (Node 1, Node 2, and Node 3), ensuring redundancy and fault tolerance. Each node stores a synchronized copy of the voting records, enabling transparency and auditability.

To maintain consistency across nodes, a consensus mechanism is employed. This mechanism ensures that all nodes agree on the validity of each transaction before it is permanently recorded in the ledger. By distributing the validation process, the system eliminates reliance on a single authority and enhances resistance to manipulation.

Finally, the recorded data is aggregated and presented through the result dashboard, which provides real-time visualization of election outcomes. This component allows administrators to monitor results transparently without compromising the integrity of the underlying data.

3.3 Consensus and Validation Mechanism

Instead of relying on computationally expensive consensus mechanisms, the system adopts a lightweight consensus protocol suitable for private environments, such as Practical Byzantine Fault Tolerance (PBFT) or a simplified voting-based consensus.
Ensures agreement among nodes before a vote is recorded
Provides fault tolerance against malicious or failed nodes
Reduces processing overhead compared to public consensus models
Vote validation is handled through automated execution logic (smart contract equivalent), which enforces rules such as:
One voter can only vote once
Only registered voters can participate
Votes cannot be modified after submission

3.3 Algorithm of the Voting Process

The voting process in the proposed system follows a structured algorithm designed to ensure secure vote submission and verification.

```
Input  : Voter_ID, Candidate_ID
Output : Recorded Vote Transaction
  Start
  Voter accesses voting interface
  System authenticates voter credentials
  IF authentication fails THEN
     Reject access
     End process
  ENDIF
    Generate Hash_ID = Hash(Voter_ID)
 Check voter status in ledger
 IF voter has already voted THEN
       Reject vote submission
       Display error message
ELSE
       Allow voter to select candidate
       Create vote transaction (Hash_ID, Candidate_ID)
       Submit transaction to smart contract
       Smart contract validates transaction
       Record transaction in distributed ledger
       Update vote count
       Confirm successful voting
ENDIF
End
```

This algorithm ensures that each voter can cast only one vote and that all voting records are securely stored within the distributed ledger. The process starts when the voter accesses the voting interface and submits login credentials. The system authenticates the voter and displays the candidate list. After the voter submits a vote, the smart contract validates voter eligibility and checks whether the voter has already voted. If the validation is successful, the vote is recorded in the private distributed ledger. Otherwise, the transaction is rejected, and the voter receives an error message.

3.4 System Implementation

The proposed system is implemented using several technologies to support decentralized voting operations. The distributed ledger environment is simulated using a private ledger network deployed on a local server. Smart contracts are used to define voting rules and manage vote transactions.

The web interface allows users to interact with the system through a simple and accessible voting platform. The interaction between the web interface and the distributed ledger is managed through an application programming interface that enables secure communication between system components.

3.5 System Testing

The system testing phase is conducted to verify the functionality and reliability of the proposed voting system. Two testing approaches are applied in this study:

1. **Functional Testing**

Functional testing is performed to ensure that each system component operates according to its intended function. The testing process includes voter registration verification, vote submission validation, prevention of duplicate voting, and vote counting accuracy.

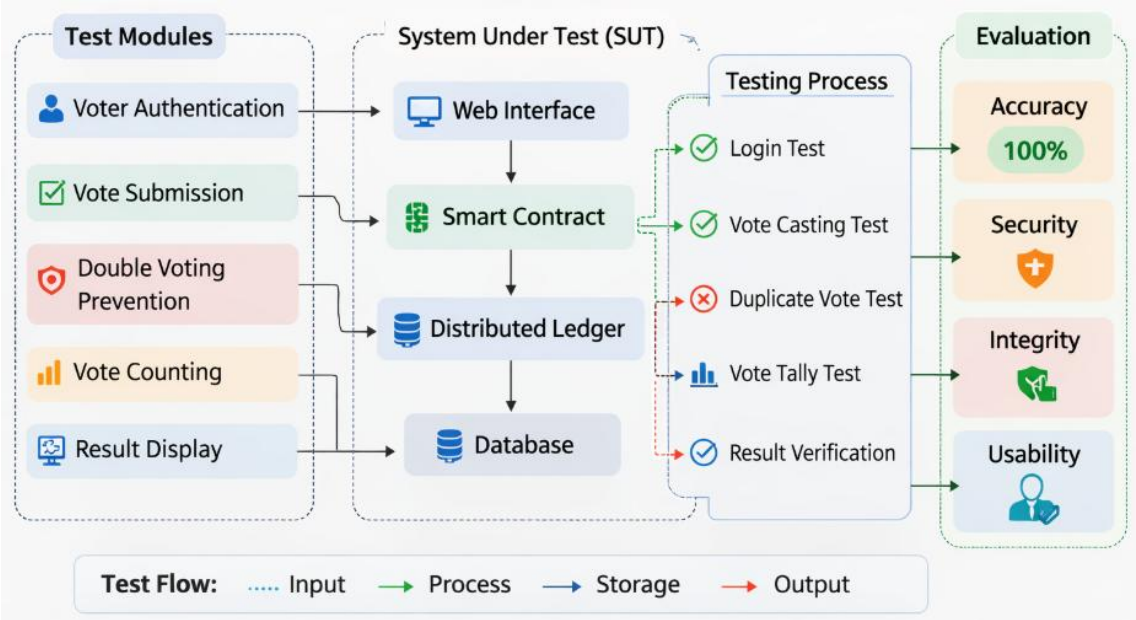

Figure 2. Functional testing workflow

The figure 2 functional testing workflow of the proposed decentralized e-voting system. The purpose of this testing phase is to verify that each functional component of the system operates according to its intended design and produces the expected outputs.

The testing process begins with the identification of several test modules, which represent the main functional components of the e-voting system. These modules include voter authentication, vote submission, duplicate vote prevention, vote counting, and result display. Each module is tested independently to ensure that the system behaves correctly in different voting scenarios.

The first test module is voter authentication, where the system verifies whether the user attempting to access the voting platform is a registered voter. The authentication process ensures that only eligible voters can access the voting interface and participate in the election process.

The second module is vote submission testing, which evaluates whether the system correctly records the vote selected by the voter. This module verifies that the selected candidate is successfully transmitted to the smart contract and stored in the distributed ledger.

The third module focuses on duplicate vote prevention. In this stage, the system checks whether the same voter attempts to submit more than one vote. The smart contract automatically validates the voter status and rejects any duplicate voting attempt, ensuring the integrity of the election process.

The fourth module is vote counting, which verifies whether the system correctly aggregates the voting transactions stored in the ledger and calculates the total number of votes received by each candidate.

The final module is result display, where the system presents the election results through the dashboard interface. This module ensures that the vote tabulation results are displayed accurately and in real time. In the diagram, the System Under Test (SUT) consists of several integrated components, including the web interface, smart contract, distributed ledger, and database. The web interface serves as the user interaction layer, the smart contract enforces voting rules, the distributed ledger records immutable voting transactions, and the database stores supporting application data. The testing process is performed through several evaluation steps, including login testing, vote casting testing, duplicate vote validation, vote tally verification, and result verification. Each test case is executed to determine whether the system produces the expected output. Finally, the evaluation stage measures several key system performance indicators, including accuracy, security, data integrity, and usability. The results show that the system achieves a high level of accuracy in vote recording and counting, maintains data integrity through immutable ledger transactions, and provides a secure and user-friendly voting interface.

Through this functional testing process, the reliability of the proposed decentralized e-voting system can be validated before deployment in a real election environment.

$$Accuracy = \frac{Number\ of\ Correct\ Results}{Total\ Number\ of\ Test\ Cases} \times 100\%$$

Variable

Correct Results : Number of passed tests or Number of successful test cases.
Total Test Cases : total number of test scenarios performed
Example :
Total Test Case = 25
Successful Test = 24

$$Accuracy = \frac{24}{25} \times 100\%$$

$$Accuracy = 96\%$$

Based on the testing results, the system achieved an accuracy rate of **96%**, indicating that the majority of system functions operated according to the expected behavior.

2. Simulation Testing

A voting simulation is conducted to evaluate the performance of the system in a realistic voting scenario. The simulation involves multiple voters and candidates in order to measure system reliability and performance.

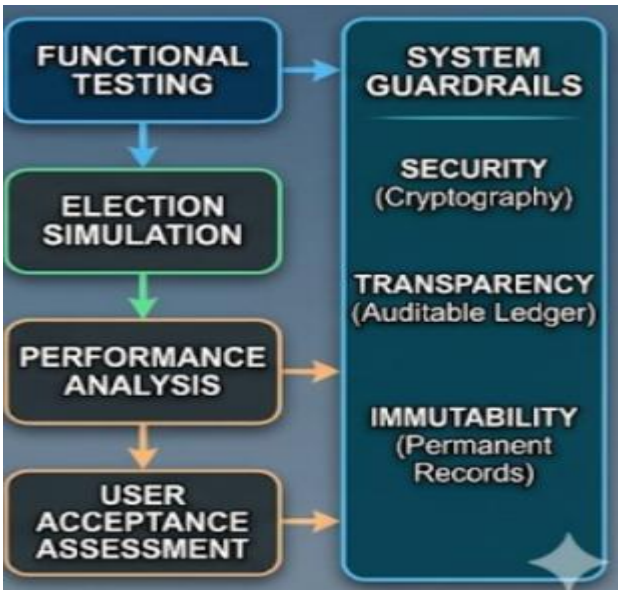

Figure 3. Simulation Framework Testing of The Proposed E-Voting System

The figure illustrates the simulation framework of the proposed decentralized e-voting system used to evaluate the functionality and performance of the developed voting platform. The framework demonstrates how different system components interact during the voting process, starting from voter interaction to vote validation and result monitoring.

The simulation environment consists of several main components: web client, smart contract module, distributed ledger network, IPFS storage, validating nodes, and the administrator dashboard.

The process begins with the web client, which acts as the voter interface. Through this interface, voters access the voting system and submit their selected candidate. Before the vote is processed, the system performs cryptographic hashing on the voter identity to protect personal information and ensure voter anonymity. The hashed voter ID is then used during the verification process to prevent duplicate voting.

Once the vote data is submitted, it is sent to the smart contract module, which contains the voting logic and rules. The smart contract verifies voter eligibility and ensures that each voter can cast only one vote. If the voting request satisfies the defined conditions, the transaction is approved and prepared for recording in the distributed ledger.

The verified vote transaction is then transmitted to the distributed ledger network, where it is validated by several validating nodes. These nodes collectively verify the transaction and add it to the ledger. Because the ledger operates using a distributed mechanism, the recorded voting data becomes immutable and transparent, ensuring that the vote cannot be modified once confirmed.

In addition to ledger recording, the system stores hashed voter identity data within the IPFS (InterPlanetary File System) module. This decentralized storage mechanism helps maintain voter privacy while enabling secure verification of voter identities without exposing personal information.

After the voting transaction has been confirmed and recorded in the ledger, the results can be retrieved by the administrator dashboard. The dashboard provides real-time monitoring of voting activity and displays aggregated election results. Administrators can observe the number of votes received by each candidate and monitor system activity during the election process.

Through this simulation framework, the study evaluates the interaction between the voting interface, smart contracts, distributed ledger infrastructure, and result monitoring mechanisms. The framework demonstrates how decentralized technologies can be integrated to provide a secure, transparent, and tamper-resistant electronic voting system.

3.6 System Evaluation

The evaluation stage focuses on measuring the effectiveness of the proposed system in terms of performance, security, and usability. The evaluation includes:

• performance analysis of system resource usage
• measurement of voting transaction efficiency
• user acceptance testing through questionnaires

The results of these evaluations provide insights into the feasibility of implementing decentralized voting systems on local server infrastructures.

4. Results and Discussions

This section presents the experimental results obtained from the implementation and evaluation of the proposed decentralized e-voting system. The evaluation focuses on three main aspects, namely functional accuracy, system performance, and user acceptance. The objective of this evaluation is to determine whether the proposed system can operate reliably and efficiently within a decentralized voting environment.

The testing process was conducted using a simulated election scenario involving 20 registered voters, three candidates, and three polling officers. The system was deployed on a local distributed ledger environment to measure the performance and functionality of the proposed voting platform.

4.1 System Performance Analysis

In addition to functional accuracy, system performance was also evaluated by measuring the transaction cost (gas usage) and system response time. These metrics are important to assess the efficiency of decentralized voting systems.

Table 1. System Performance Evaluation

Transaction Type	Average Gas Usage	Response Time (seconds)	Status
Voter Authentication	21,000	0.8	Success
Vote Submission	45,200	1.4	Success
Smart Contract Validation	37,500	1.2	Success
Ledger Recording	52,800	1.6	Success
Vote Counting	28,300	0.9	Success
Result Display	15,200	0.6	Success

From the results shown in Table 1. Although the system demonstrates efficient response times (0.6–1.6 seconds), these results should be interpreted within the context of a controlled environment. Compared to previous distributed e-voting systems that rely on public infrastructures, which often experience higher latency due to network congestion and transaction validation overhead, the proposed system benefits from a locally managed environment that reduces communication delays.

However, unlike large-scale implementations discussed in prior studies, this evaluation was conducted with only 20 simulated voters. Therefore, the results primarily demonstrate system feasibility rather than scalability. Previous research has shown that distributed voting systems may encounter performance degradation under high transaction loads, particularly in terms of throughput and synchronization delay. This limitation indicates that further large-scale performance testing is required before the system can be considered suitable for broader deployment.

4.2 User Acceptance Testing (UAT)

User Acceptance Testing was conducted to evaluate the usability and user experience of the proposed voting system. A questionnaire-based evaluation was distributed to 30 participants who simulated the voting process.

The evaluation consisted of several criteria including ease of use, system reliability, security perception, and interface usability.

Table 2. User Acceptance Testing Results

Evaluation Criteria	Strongly Agree	Agree	Neutral	Disagree
System is easy to use	12	6	2	0

Voting process is clear	13	5	2	0
System is secure	11	7	2	0
Interface is user-friendly	10	8	2	0

From table 2 The user acceptance results indicate a generally positive perception of system usability, with an average acceptance rate of 92%. However, the interpretation of these results should be approached with caution. The sample size of 30 participants is relatively small and may not represent diverse user groups. In addition, the analysis is limited to descriptive statistics without inferential validation, which restricts the generalizability of the findings.

Compared to previous studies, where usability evaluation is often overlooked, this study contributes by incorporating user-centered assessment. Nevertheless, the absence of statistical analysis and participant diversity suggests that the usability findings should be considered preliminary.

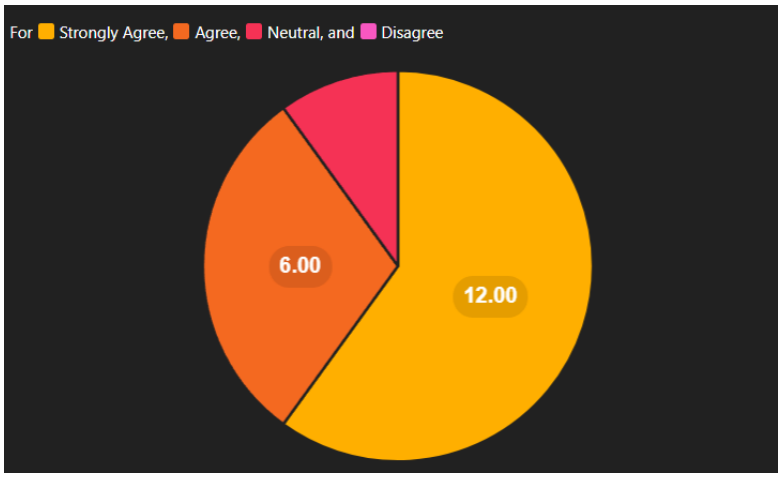

Figure 4. User Acceptance Testing Results

The pie chart illustrates the results of the **User Acceptance Testing (UAT)** conducted with 20 participants. The evaluation measures the user perception regarding system usability, clarity of the voting process, and perceived security.

Based on the collected responses:

60% of respondents strongly agree that the system is easy to use.

30% agree that the voting process is clear and understandable.

10% remain neutral regarding the usability of the interface.

0% disagree, indicating that no participants reported negative experiences while interacting with the system.

These results indicate that the proposed decentralized e-voting platform provides a **user-friendly interface and a clear voting workflow**, which contributes to positive user perception and system acceptance

4.3 System Performance Analysis

The system performance was evaluated by measuring the response time required for each major transaction in the voting process. The bar chart shows the average response time for several system operations including authentication, vote submission, smart contract validation, ledger recording, vote counting, and result display.

The results indicate that:

Authentication requires approximately 0.8 seconds
Vote submission requires about 1.4 seconds
Smart contract validation takes approximately 1.2 seconds
Ledger transaction recording takes around 1.6 seconds
Vote counting requires approximately 0.9 seconds
Result display takes approximately 0.6 seconds

The average response time for all system operations remains below two seconds, indicating that the system is capable of processing voting transactions efficiently within a decentralized environment.

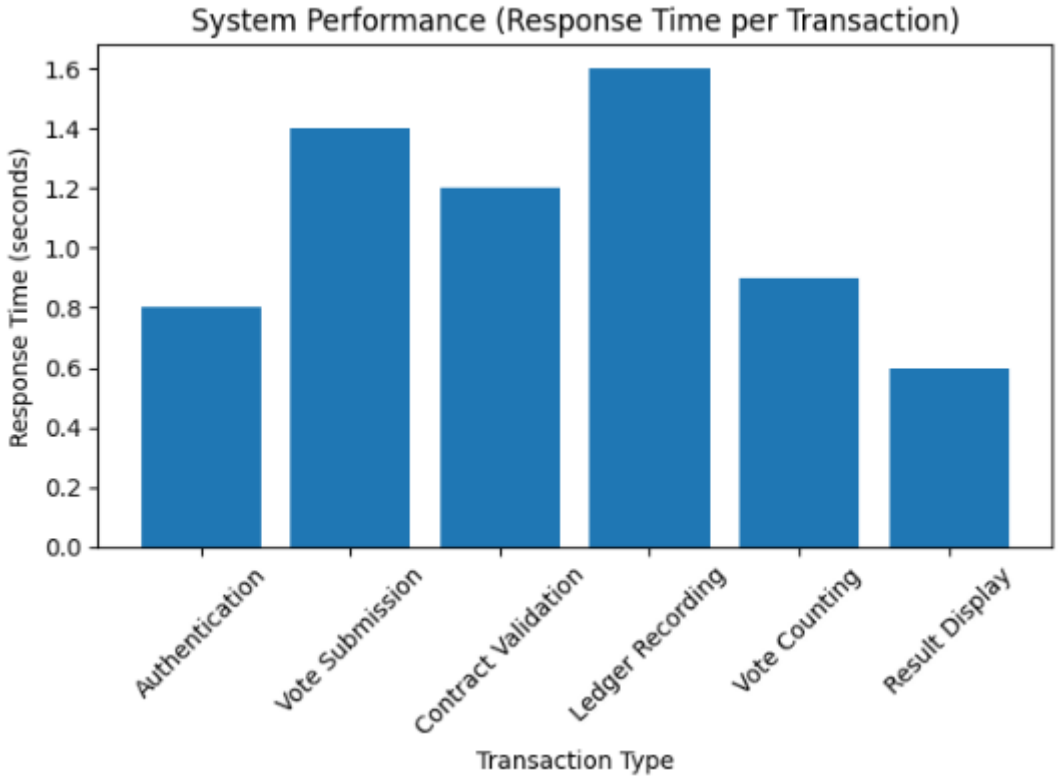

Figure 5. System performance evaluation based on transaction response time

The experimental results demonstrate that the proposed decentralized e-voting system achieves high levels of usability and operational efficiency. The user acceptance results indicate that the majority of participants perceive the system as easy to use and reliable. Furthermore, the system performance evaluation shows that voting transactions can be processed quickly with minimal latency. These findings suggest that the proposed system is capable of supporting secure and efficient digital elections while maintaining user-friendly interaction and reliable system performance.

Positioning of Novelty

The novelty of this study lies in its attempt to move beyond purely conceptual decentralized voting proposals by implementing and evaluating a working system in a local infrastructure context. While previous studies have extensively discussed secure vote recording, distributed validation, and transparency mechanisms, fewer works have focused on how these principles can be operationalized in environments where performance efficiency, administrative control, and practical deployment constraints are equally important (Daramola & Thebus, 2020; Daraghmi et al., 2024). By demonstrating good functional reliability and low response time in a controlled distributed environment, this study contributes to the emerging line of research that seeks to balance decentralization with real-world feasibility.

5. Conclusion

This study proposed and implemented a decentralized electronic voting system based on distributed ledger technology to enhance the security, transparency, and efficiency of digital election processes. The system integrates a web-based voting interface, smart contract validation mechanisms, and a distributed ledger infrastructure to ensure that each voting transaction is securely recorded and cannot be modified after confirmation. The experimental results demonstrate that the proposed system achieved a functional testing accuracy of **96%**, while the average transaction response time remained **below two seconds**, indicating efficient system performance within the simulated voting environment. Furthermore, the user acceptance evaluation shows that the majority of respondents perceive the system as easy to use and reliable, highlighting its potential usability in real-world applications. The main contribution of this research lies in the integration of decentralized technologies with a practical voting interface and a comprehensive evaluation framework that includes functional testing, performance analysis, and user acceptance assessment. These findings suggest that decentralized voting platforms can serve as a viable alternative to conventional electronic voting systems by improving trust, transparency, and data integrity. Future research may focus on scaling the system for larger election environments, improving network efficiency, and exploring additional security mechanisms to further strengthen the reliability of decentralized voting infrastructures.

Acknowledgement

This research was supported/partially supported by Universitas Harapan Medan, thank our colleagues from Universiti Malaysia Perlis who provided insight and expertise that greatly assisted the research, although they may not agree with all of the interpretations/conclusions of this paper.

References

Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. (2020, October). Decentralized E-voting system based on Smart Contract by using Blockchain Technology. In *2020 international conference on smart innovations in design, environment, management, planning and computing (ICSIDEMPC)* (pp. 176-180). IEEE. https://ieeexplore.ieee.org/document/9299581

Almeida, R. L., Baiardi, F., Maesa, D. D. F., & Ricci, L. (2023). Impact of decentralization on electronic voting systems: A systematic literature survey. *IEEE Access, 11*, 132389-132423. https://ieeexplore.ieee.org/document/10328599

Ali, H. M. (2025). A Systematic Review of Digital Authentication for Blockchain-Based E-Voting Systems. *Iraqi Journal of Intelligent Computing and Informatics (IJICI)*, *4*(2), 250-259.

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for E-voting: a systematic literature review. *IEEE Access, 10*, 70746-70759. https://ieeexplore.ieee.org/document/9812616

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). Blockchain-based e-voting systems: a technology review. *Electronics, 13*(1), 17. https://www.mdpi.com/2079-9292/13/1/17

Brasser, C. (2021). *Design and Implementation of Systems Interfaces for a Decentralized Remote Electronic Voting System* (Doctoral dissertation, MS thesis, University of Zurich).

Daraghmi, E., Hamoudi, A., & Abu Helou, M. (2024). Decentralizing democracy: Secure and transparent e-voting systems with distributed ledger technology. *Future Internet, 16*(11), 388. https://www.mdpi.com/1999-5903/16/11/388

Daramola, O., & Thebus, D. (2020). Architecture-centric evaluation of blockchain-based smart contract e-voting for national elections. *Informatics, 7*(2), 16. https://www.mdpi.com/2227-9709/7/2/16

Fatih, R., Arezki, S., & Gadi, T. (2023). A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings. *International Journal of Interactive Mobile Technologies, 17*(23).

Gupta, V. K., Jain, P., Agarwal, S., Shukla, V., & Goel, N. (2025, March). Electronic Voting System Using Blockchain Technology. In *2025 3rd International Conference on Disruptive Technologies (ICDT)* (pp. 401-407). IEEE.

Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018, July). E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1561-1567). IEEE.

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. *Sensors*, *21*(17), 5874. https://www.mdpi.com/1424-8220/21/17/5874

Jumaa, M. H., & Shakir, A. C. (2023). Review study of e-voting system based on smart contracts using blockchain technology. *Iraqi Journal of Science*, 2001-2022.

Khan, K. M., et al. (2022). Blockchain-based secure e-voting systems: Challenges and opportunities.

Kusi, A., & Asoma, D. (2025). Blockchain-Based E-Voting Systems: A Systematic Literature Review on Privacy, Integrity, and Scalability. *Integrity, and Scalability* (July 17, 2025).

Marouan, A., Badrani, M., Zannou, A., & Kannouf, N. (2025). Blockchain-based e-voting for university elections. *SN Computer Science*, *6*(3), 204.

Mookherji, S., Vanga, O., & Prasath, R. (2022). Blockchain-based e-voting protocols. In *Blockchain Technology for Emerging Applications* (pp. 239-266). Academic Press.

Ohize, H. O., Onumanyi, A. J., Umar, B. U., Ajao, L. A., & Isah, R. O. (2025). Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing*, *28*(2), 132. https://link.springer.com/article/10.1007/s10586-024-04709-8

Patra, A., Basu, S., & Majumder, K. (2025). Blockchain-enabled secured and transparent e-voting system using smart contracts. *International Journal of Next-Generation Computing*, *16*(1), 1–17.

Prasad, S. S., Vardhini, P. H., Sai, M. V., Raju, K. M., & Jyothi, K. (2024, March). Identification of Gender from the Shortest Speech using Hybrid and Optimised Spectral Features using Machine Learning Model. In *2024 IEEE International Conference on Contemporary Computing and Communications (InC4)* (Vol. 1, pp. 1-7). IEEE. https://doi.org/10.1109/ICBDS61829.2024.10837039

Singh, A., Ganesh, A., Patil, R. R., Kumar, S., & Rani, R. (2023). Secure voting website using Ethereum and smart contracts. *Applied System Innovation*, *6*(4), 70. https://www.mdpi.com/2571-5577/6/4/70

Spanos, A., & Kantzavelou, I. (2025). EtherVote: a secure smart contract-based e-voting system. *Wireless Networks*, *31*(2), 1279-1299. https://link.springer.com/article/10.1007/s11276-024-03818-x

Tang, W., Yang, W., Tian, X., & Yuan, S. (2023). Distributed anonymous e-voting method based on smart contract authentication. *Electronics*, *12*(9), 1968. https://www.mdpi.com/2079-9292/12/9/1968

Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-voting meets blockchain: A survey. *IEEE Access*, *11*, 23293-23308. https://ieeexplore.ieee.org/document/10061373