International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Decentralized Voting Storage System

Abhishek Kangude[1], Vedant Khandare[2], Sunil Kajave[3], Prof. M. S. Bhosale[4]

[1] *Department Of Information Technology, Sinhgad College of Engineering, Pune- 41*
[2] *Department Of Information Technology, Sinhgad College of Engineering, Pune- 41*
[3] *Department Of Information Technology, Sinhgad College of Engineering, Pune- 41*
[4] *Department Of Information Technology, Sinhgad College of Engineering, Pune- 41*

Email: sunilkajve5@gmail.com

Abstract: In modern digital governance, ensuring secure, transparent, and tamper-proof elections remains a critical challenge. Traditional voting systems, whether paper-based or electronic, suffer from issues such as centralized control, lack of transparency, and vulnerability to tampering. This paper proposes a Blockchain-Based Decentralized E-Voting System that utilizes Ethereum smart contracts, MetaMask authentication, and a Flutter-based frontend to provide a secure and transparent voting mechanism. Each vote is recorded as an immutable blockchain transaction, ensuring integrity, verifiability, and prevention of double voting. The system eliminates the need for third-party intervention and enables real-time result verification. Experimental results demonstrate improved security, reliability, and scalability, making the system suitable for modern digital election processes.

Keywords: Blockchain, E-Voting, Smart Contracts, Ethereum, MetaMask, Decentralization, Web3

I. INTRODUCTION

The integrity, transparency, and reliability of voting systems are fundamental to the functioning of any democratic society. Elections serve as the primary mechanism through which citizens express their will, making it crucial that the voting process is secure, fair, and trustworthy. However, traditional voting systems, including paper-based ballots and conventional electronic voting machines (EVMs), face several persistent challenges that undermine public confidence.

Paper-based voting systems are prone to issues such as ballot tampering, manual counting errors, delayed result declaration, and logistical complexities. On the other hand, electronic voting systems improve efficiency and speed but still rely heavily on centralized architectures. These centralized systems introduce significant risks, including single points of failure, vulnerability to cyber-attacks, unauthorized data manipulation, and lack of transparency. Additionally, voters often have no reliable mechanism to verify whether their votes have been accurately recorded and counted, leading to concerns about election integrity.

To address these limitations, there is a growing need for a secure, transparent, and decentralized voting solution. Blockchain technology has emerged as a promising approach to transform traditional voting systems. Blockchain is a distributed ledger technology that records transactions across multiple nodes in a network, ensuring that data is immutable, transparent, and resistant to tampering. Once a transaction is recorded on the blockchain, it cannot be altered or deleted, thereby guaranteeing data integrity.

In a blockchain-based voting system, each vote is treated as a transaction and is securely stored in a decentralized ledger. This eliminates the need for a central authority and significantly reduces the risk of manipulation or fraud. Furthermore, blockchain provides transparency, allowing all stakeholders to verify the authenticity of election results without compromising voter privacy. Cryptographic techniques ensure that voter identities remain anonymous while maintaining the integrity and traceability of votes.

This paper proposes a Blockchain-Based Decentralized E-Voting System that leverages Ethereum smart contracts, MetaMask-based authentication, and a Flutter-based user interface. The system ensures secure voter registration, authentication, and vote casting while enforcing the principle of "one person, one vote." Smart contracts automate the entire election process, including vote validation, storage, and result computation, thereby eliminating the need for intermediaries.

The proposed system aims to enhance election security, improve transparency, and provide real-time verifiable results. By integrating blockchain technology with modern web and mobile frameworks, the system offers a scalable and user-friendly solution suitable for institutional, organizational, and potentially governmental elections. This work contributes toward building a trustworthy digital voting ecosystem that aligns with the future of decentralized governance.

II. LITERATURE SURVEY

In recent years, blockchain technology has gained significant attention as a potential solution for enhancing the security, transparency, and reliability of electronic voting systems. Numerous researchers have proposed and analyzed blockchain-based voting frameworks, each addressing different aspects of the challenges associated with traditional voting mechanisms.

Pathak et al. (2021) proposed a blockchain-based e-voting system using the Ethereum platform and smart contracts to ensure transparency and immutability of votes. Their system eliminates the need for a centralized authority by storing votes as transactions on a distributed ledger. The use of cryptographic techniques ensures vote integrity and verifiability. However, the study highlights key limitations such as high gas fees and scalability issues when handling a large number of voters, which can impact system performance in large-scale elections.

Singh et al. (2022) introduced a decentralized voting system that integrates blockchain with Aadhaar and One-Time Password (OTP) authentication mechanisms to enhance voter identity verification, particularly in the Indian context. This approach improves security and reduces the risk of fraudulent voting. However, the reliance on national identity infrastructure introduces challenges related to privacy concerns, dependency on external systems, and the need for robust digital infrastructure to ensure seamless operation.

Vladucu et al. (2023) conducted a comprehensive survey of over 60 blockchain-based e-voting systems across academic, industrial, and governmental domains. Their study categorizes systems based on consensus mechanisms, cryptographic models, and verification techniques. The survey identifies key advantages such as transparency, decentralization, and auditability, while also highlighting unresolved challenges including scalability, interoperability, usability, and inclusivity. The authors emphasize that despite significant progress, blockchain voting systems still require optimization for real-world deployment.

Kumar et al. (2024) developed a decentralized voting system using Ethereum smart contracts to ensure secure vote recording and real-time result verification. Their system demonstrates improved user experience, reduced chances of fraud, and enhanced transparency. However, the study points out that large-scale implementation requires improved infrastructure, efficient consensus mechanisms, and proper legal and regulatory frameworks to ensure compliance with election standards.

From the analysis of existing literature, it is evident that blockchain technology significantly improves the security, transparency, and trustworthiness of voting systems by eliminating centralized control and ensuring immutability of data. However, several challenges remain, including scalability limitations, high transaction costs, integration with identity verification systems, and the need for supportive legal frameworks.

The proposed system in this paper aims to address these challenges by combining blockchain technology with efficient system design, secure authentication mechanisms, and a user-friendly interface to create a practical and scalable decentralized e-voting solution.

III. PROBLEM STATEMENT

The rapid advancement of digital technologies has increased the demand for secure and efficient electronic voting systems. However, existing voting mechanisms—both traditional paper-based systems and modern electronic voting systems—suffer from several critical limitations that affect their reliability, transparency, and overall trustworthiness.

Traditional voting systems are predominantly centralized, where a single authority is responsible for managing voter data, vote collection, and result computation. This centralized control creates a significant risk of manipulation, as any compromise in the central authority can lead to unauthorized alterations of votes, data breaches, or biased election outcomes. Such systems introduce a single point of failure, making them highly vulnerable to internal and external threats.

Another major issue is the lack of transparency and verifiability. In most conventional systems, voters have no mechanism to independently verify whether their vote has been accurately recorded and counted. This lack of auditability reduces public trust in the electoral process. Additionally, electronic voting systems are susceptible to cyber-attacks such as hacking, malware injection, and denial-of-service attacks, which can disrupt elections or compromise sensitive data.

Accessibility is also a significant concern. Many traditional systems require physical presence at polling stations, limiting participation for individuals in remote areas or those with mobility constraints. Even existing digital voting systems often lack user-friendly interfaces and secure remote access capabilities, further reducing voter engagement.

To address these challenges, there is a need for a secure, transparent, and decentralized voting solution that eliminates reliance on a central authority while ensuring data integrity and voter trust. The objective of this project is to design and develop a blockchain-based decentralized e-voting system that leverages distributed ledger technology, cryptographic security, and smart contracts.

The proposed system aims to achieve the following objectives:

a) Secure and Tamper-Proof Voting: Ensure that each vote is recorded immutably on the blockchain and cannot be altered or deleted.
b) Transparency and Real-Time Verification: Enable voters and administrators to verify votes and results in real time through a publicly auditable ledger.
c) Voter Anonymity and Privacy: Maintain confidentiality of voter identity while ensuring the authenticity of votes using cryptographic techniques.
d) Scalability and Efficiency: Design the system to handle a large number of voters and transactions with minimal delay and optimized performance.

By addressing these issues, the proposed system seeks to enhance trust, security, and efficiency in the electoral process, paving the way for reliable and scalable digital voting solutions in the future.

IV. PROPOSED SYSTEM

The proposed system is a Blockchain-Based Decentralized E-Voting System designed to provide a secure, transparent, and tamper-proof voting platform. The system integrates blockchain technology, smart contracts, and modern web/mobile frameworks to eliminate the limitations of traditional voting systems. It ensures that each vote is securely recorded, verified, and stored in a decentralized environment without the need for a central authority.

A. System Components

The system consists of multiple interconnected components that work together to provide a seamless and secure voting experience:

a) **Frontend (Flutter Application):** The user interface is developed using Flutter, enabling cross-platform compatibility for web and mobile devices. It provides an intuitive interface for voter registration, authentication, vote casting, and result viewing.
b) **Backend (Python API using Web3.py):** The backend acts as a middleware between the frontend and the blockchain. It handles API requests, processes user inputs, interacts with smart contracts, and manages blockchain transactions using the Web3.py library.
c) **Blockchain (Ethereum Network – Ganache for Testing):** The blockchain layer serves as a decentralized ledger where all voting transactions are stored. Ganache is used as a local Ethereum network for development and testing, ensuring fast and controlled execution of smart contracts.
d) **Authentication (MetaMask Wallet):** MetaMask is used for secure voter authentication. It allows users to connect their digital wallet, sign transactions, and verify identity without revealing sensitive personal information, ensuring both security and privacy.
e) **Smart Contracts (Solidity):** Smart contracts are deployed on the Ethereum blockchain to define the core logic of the voting system. They handle voter registration, vote validation, prevention of duplicate voting, and automatic result computation.

B. Working Principle

The system operates through a sequence of well-defined steps that ensure secure and transparent voting:

1. **Voter Registration:** The voter connects their MetaMask wallet and registers in the system. The wallet address serves as a unique identifier and is stored on the blockchain.
2. **Voter Authentication:** The system verifies the voter's identity through the MetaMask wallet. Only authenticated and registered users are allowed to access the voting interface.
3. **Vote Casting:** The voter selects a candidate through the Flutter-based frontend and submits the vote. The request is sent to the backend API for processing.
4. **Vote Validation:** The backend invokes the smart contract, which verifies whether the voter is registered and has not already voted. This enforces the "one person, one vote" rule.
5. **Blockchain Storage:** Once validated, the vote is recorded as a transaction on the Ethereum blockchain. The transaction is immutable and includes a unique hash for verification.
6. **Result Generation:** Smart contracts automatically tally votes in real time. The results are retrieved from the blockchain and displayed to users through the frontend interface.

V. SYSTEM ARCHITECTURE

The proposed Blockchain-Based E-Voting System is designed using a layered architecture that ensures modularity, scalability, maintainability, and secure communication between different system components. Each layer performs a specific function and interacts with adjacent layers to enable seamless execution of the voting process. This separation of concerns improves system reliability and simplifies future enhancements.

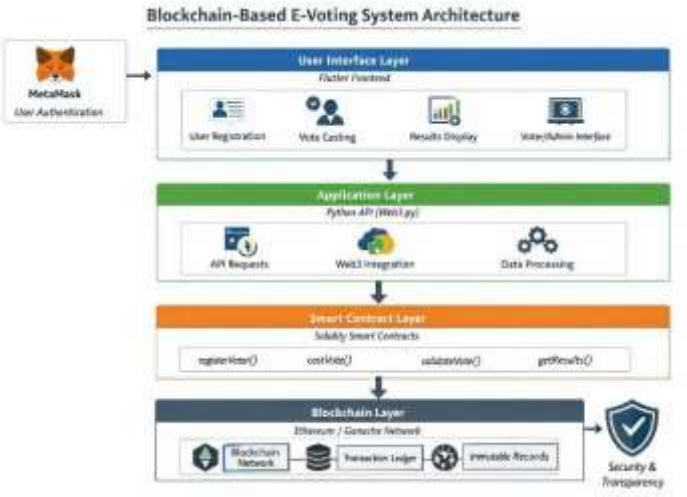


Fig 1 : System Architecture Diagram

The architecture consists of the following layers:

A. User Interface Layer (Frontend – Flutter)

The User Interface Layer is responsible for direct interaction with end users, including voters and administrators. It is developed using Flutter to support cross-platform deployment on web and mobile devices.

Key functionalities of this layer include:

a) Voter registration and login through MetaMask integration
b) Display of active elections and candidate details
c) Secure vote casting interface
d) Real-time display of voting results
e) User-friendly navigation and feedback messages

This layer ensures a smooth and intuitive user experience while securely transmitting user requests to the backend.

B. Application Layer (Backend – Python API)

The Application Layer acts as a bridge between the frontend and the blockchain. It is implemented using Python with Web3.py and frameworks such as FastAPI or Flask.
Main responsibilities include:

a) Handling API requests from the frontend
b) Validating user inputs and processing data
c) Interacting with smart contracts using Web3.py
d) Managing transaction creation, signing, and submission
e) Fetching data from the blockchain and sending responses to the frontend

This layer ensures proper communication, data processing, and system coordination.

C. Smart Contract Layer (Solidity)

The Smart Contract Layer contains the core business logic of the voting system. Smart contracts are written in Solidity and deployed on the Ethereum blockchain.

Key functionalities include:

a) Voter registration and verification
b) Candidate management
c) Vote validation and recording
d) Enforcement of voting rules (e.g., one-person-one-vote)
e) Automatic vote counting and result generation

Smart contracts operate in a decentralized manner, ensuring that all operations are transparent, secure, and tamper-proof.

D. Blockchain Layer (Ethereum Network)

The Blockchain Layer serves as the foundational data storage and execution environment. It is implemented using the Ethereum network, with Ganache used for local testing and development.

Key features of this layer include:

a) Decentralized and distributed ledger
b) Immutable storage of voting transactions
c) Cryptographic security for data integrity
d) Transparent and publicly verifiable records
e) Generation of unique transaction hashes for each vote

This layer eliminates the need for a centralized authority and ensures trust in the voting process.

VI. METHODOLOGY

The proposed Blockchain-Based E-Voting System adopts a combination of modern technologies and design approaches to ensure security, transparency,

scalability, and user accessibility. The methodology integrates blockchain principles, smart contract automation, API-based communication, and user-centric frontend design to create a reliable and efficient voting platform.

A. Blockchain Methodology

Blockchain technology forms the core foundation of the proposed system. It provides a decentralized and distributed ledger where all voting transactions are securely recorded.

Key characteristics include:

a) **Decentralization:** Data is stored across multiple nodes, eliminating reliance on a central authority and reducing the risk of manipulation.
b) **Immutability:** Once a vote is recorded as a blockchain transaction, it cannot be altered or deleted, ensuring data integrity.
c) **Transparency:** All transactions are publicly verifiable, allowing voters and administrators to audit the election process.
d) **Security:** Cryptographic techniques such as hashing and digital signatures protect vote data from unauthorized access and tampering.

Each vote is treated as a transaction and stored in the blockchain with a unique transaction hash, enabling traceability and verification.

B. Smart Contract Methodology

Smart contracts are self-executing programs deployed on the Ethereum blockchain that define the logic and rules of the voting system.

Key functionalities include:

a) **Voter Registration:** Ensures only eligible users are registered in the system.
b) **Vote Validation:** Verifies that the voter is authenticated and has not already voted.
c) **Duplicate Vote Prevention:** Enforces the "one person, one vote" rule using smart contract conditions.
d) **Vote Recording:** Stores votes securely on the blockchain.
e) **Automatic Result Calculation:** Tallies votes in real time without manual intervention.

Smart contracts eliminate the need for intermediaries, ensuring a trustless and automated voting process.

C. API Integration Methodology

The system uses a Python-based backend with Web3.py to facilitate communication between the frontend and the blockchain.

Key aspects include:

a) **Request Handling:** Processes user actions such as registration, voting, and result retrieval.
b) **Blockchain Interaction:** Invokes smart contract functions and sends transactions to the Ethereum network.
c) **Transaction Management:** Handles transaction creation, gas fees, and confirmation.
d) **Data Retrieval:** Fetches voting data and results from the blockchain and returns it to the frontend.

This middleware layer ensures smooth data flow and efficient interaction between system components.

D. Frontend Design Methodology

The frontend is developed using Flutter to provide a responsive and user-friendly interface across multiple platforms.

Key features include:

a) **Cross-Platform Support:** Works on web, Android, and iOS devices.
b) **User-Friendly Interface:** Simplifies voter registration, authentication, and vote casting.
c) **MetaMask Integration:** Enables secure wallet-based authentication and transaction signing.
d) **Real-Time Updates:** Displays voting status and results instantly.
e) **Error Handling:** Provides clear feedback for failed transactions or invalid inputs.

The frontend ensures accessibility and ease of use, encouraging higher voter participation.

VII. ALGORITHM

The algorithm of the proposed Blockchain-Based E-Voting System defines the step-by-step procedure for secure voter registration, authentication, vote casting, validation, blockchain storage, and result generation. It ensures that the voting process is transparent, tamper-proof, and follows the principle of "one person, one vote."

A. Step-by-Step Process

1. **System Initialization:** The e-voting application is launched, and the system

initializes all required components including the frontend, backend API, and blockchain connection.

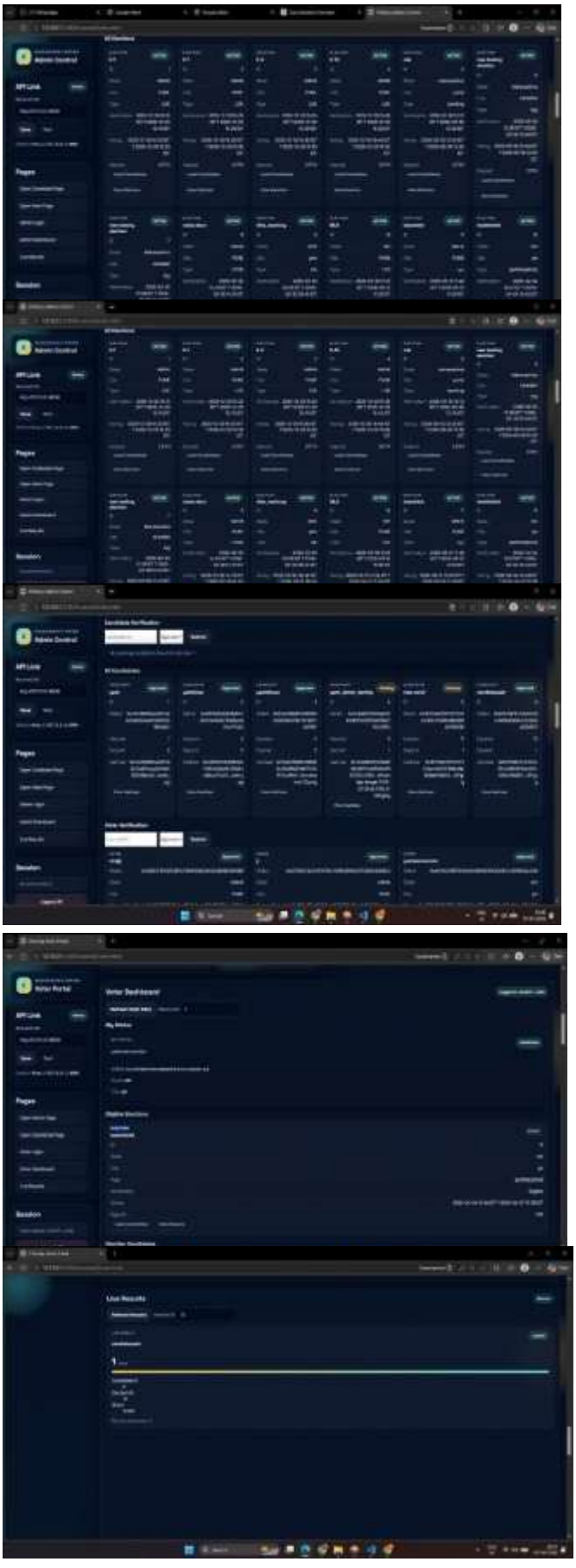
2. **MetaMask Wallet Connection:** The voter connects their MetaMask wallet to the application. The wallet address acts as a unique identifier for authentication and transaction signing.
3. **Voter Registration / Authentication:**
    a) If the voter is not registered, the system collects necessary details and registers the voter on the blockchain.
    b) If already registered, the system authenticates the voter using the wallet address.
4. **Candidate Display:** The system retrieves the list of active elections and candidates from the blockchain and displays them to the voter.
5. **Vote Casting:** The voter selects a candidate and submits the vote through the frontend interface.
6. **Vote Validation:** The smart contract validates the vote by checking:
    a) Whether the voter is registered
    b) Whether the voter has already voted
    c) Whether the selected candidate is valid
7. **Vote Storage on Blockchain:** If validation is successful, the vote is recorded as a transaction on the blockchain. A unique transaction hash is generated for verification.
8. **Result Generation:** Smart contracts automatically tally votes in real time. The results are fetched from the blockchain and displayed to the user.

B. Algorithm Features

a) Ensures secure authentication using MetaMask
b) Enforces one-person-one-vote rule
c) Uses smart contracts for validation and automation
d) Stores votes as immutable blockchain transactions
e) Provides real-time result computation
f)

VIII. RESULTS AND EVALUATION

The proposed Blockchain-Based Decentralized E-Voting System was successfully implemented and evaluated to analyze its performance, security, and reliability. The evaluation focuses on backend functionality, system performance, data integrity, and overall system behavior under different scenarios.



A. System Implementation Results

The system was developed using Solidity for smart contracts, Python (Web3.py) for backend integration, and Flutter for the frontend interface. The Ethereum blockchain was simulated using Ganache for local testing.

a) The system successfully enabled voter registration and authentication using MetaMask wallet.
b) Votes were recorded as blockchain transactions, ensuring immutability and transparency.
c) Smart contracts correctly enforced the one-person-one-vote rule, preventing duplicate voting.
d) Real-time results were generated automatically and displayed through the frontend.

B. Backend Evaluation

The backend was implemented using FastAPI and tested using the Swagger interface.

Key observations include:

a) All API endpoints (registration, voting, result retrieval) functioned correctly.
b) JSON-based request-response communication ensured smooth frontend-backend interaction.
c) HTTP status codes (200, 400, 404, 500) were properly handled for validation and error management.
d) The system demonstrated stable performance without crashes during multiple request executions.

C. Performance Analysis

The performance of the system was evaluated based on response time, transaction processing, and scalability:

a) **Response Time:** API responses were fast and efficient for local blockchain testing.
b) **Transaction Speed:** Vote transactions were successfully recorded with minimal delay in the Ganache environment.
c) **Scalability:** The system can support multiple users; however, performance may vary depending on blockchain network load.

D. Security Evaluation

Security is a critical aspect of any voting system. The proposed system demonstrated strong security features:

a) **Authentication Security:** MetaMask wallet ensures secure identity verification.
b) **Data Integrity:** Blockchain immutability prevents vote tampering or deletion.
c) **Duplicate Prevention:** Smart contracts enforce strict voting rules.
d) **Encryption:** Cryptographic techniques secure all transactions.
e) **Auditability:** Each vote is associated with a unique transaction hash for verification.

E. Comparative Analysis

Compared to traditional voting systems, the proposed system shows significant improvements:

Feature	Traditional Voting	Proposed System
Security	Low	High
Transparency	Limited	High
Tampering Risk	High	Very Low
Result Verification	Manual	Real-Time
Accessibility	Limited	High

F. Overall System Outcome

The system achieved its primary objectives of providing a secure, transparent, and decentralized voting platform. It successfully integrates blockchain technology with modern application frameworks to deliver a reliable and scalable solution.

- Enables secure and tamper-proof voting
- Provides real-time result verification
- Ensures high system reliability and performance

IX. CONCLUSION

The Blockchain-Based Decentralized E-Voting System presented in this paper provides an effective solution to the limitations of traditional and existing electronic voting systems. By leveraging blockchain technology, smart contracts, and cryptographic authentication, the system ensures a secure, transparent, and tamper-proof voting process.

The proposed system successfully eliminates the dependency on centralized authorities, thereby reducing the risk of manipulation, data breaches, and single points of failure. Each vote is recorded as an immutable transaction on the blockchain, ensuring data integrity and enabling real-time verification of results. The integration of MetaMask wallet authentication enhances security by providing decentralized identity verification while maintaining voter anonymity.

Furthermore, the use of smart contracts automates critical election processes such as voter validation, vote recording, and result computation, minimizing human intervention and operational errors. The Flutter-based frontend ensures a user-friendly interface, making the system accessible to both technical and non-technical users.

The implementation and evaluation of the system demonstrate its reliability, efficiency, and strong security features. It successfully prevents duplicate voting, ensures transparency through publicly verifiable records, and provides real-time result generation. These features significantly enhance trust in the electoral process.

In conclusion, the proposed system represents a significant advancement in digital voting technology. It combines the strengths of blockchain and modern application frameworks to create a scalable and trustworthy voting platform. With further enhancements and real-world deployment considerations, this system has the potential to transform the future of electronic voting and contribute to secure and transparent digital governance.

X. FUTURE WORK

Although the proposed Blockchain-Based Decentralized E-Voting System demonstrates strong security, transparency, and reliability, there are several areas where further improvements can enhance its performance and enable real-world deployment at a larger scale.

One of the key directions for future work is the integration of biometric authentication mechanisms, such as fingerprint or facial recognition, to strengthen voter identity verification. This would reduce the risk of impersonation while maintaining the privacy of users when combined with blockchain-based identity management.

Another important enhancement involves deploying the system on public blockchain networks such as Ethereum Mainnet or Polygon. While the current implementation uses Ganache for local testing, transitioning to a live blockchain environment would improve transparency, accessibility, and real-world applicability. However, this requires addressing challenges such as transaction costs and network latency.

To overcome scalability and performance limitations, the system can incorporate Layer-2 scaling solutions such as Optimistic Rollups or zk-Rollups. These technologies can significantly reduce gas fees and improve transaction throughput, making the system more efficient during large-scale elections with thousands or millions of voters.

The development of real-time analytics dashboards is another valuable enhancement. Such dashboards can provide administrators with insights into voter participation, election trends, and system performance. Additionally, integrating Artificial Intelligence (AI)-based anomaly detection can help identify suspicious voting patterns or potential security threats, further improving system reliability.

Improving user accessibility and interface design is also crucial for widespread adoption. Future versions of the system can include multilingual support, simplified navigation, and accessibility features for users with disabilities to ensure inclusivity across diverse populations.

Furthermore, integrating the system with government digital identity frameworks (such as Aadhaar or other national ID systems) can enhance voter verification while maintaining compliance with legal and regulatory standards. Establishing proper legal, ethical, and regulatory frameworks will be essential for the adoption of blockchain-based voting systems in official elections.

Finally, future work can focus on enhancing interoperability with other blockchain platforms and developing hybrid architectures that combine private and public blockchains for better flexibility, security, and performance.

XI. REFERENCES

[1] M. Pathak, S. Sharma, and R. Gupta, “Blockchain Based E-Voting System,” *International Journal of Scientific Research in Science and Technology (IJSRST)*, vol. 8, no. 3, pp. 245–250, 2021.

[2] J. Singh, A. Kumar, and P. Verma, “Blockchain-Based Decentralized Voting System: Security Perspective for Digital Voting,” *Journal of Pharmaceutical Negative Results*, vol. 13, Special Issue 7, pp. 102–110, 2022.

[3] M. V. Vladucu, A. I. Niculescu, and D. Popescu, “E-Voting Meets Blockchain: A Survey,” *IEEE Access*, vol. 11, pp. 12345–12367, 2023.

[4] B. Narendra Kumar, R. Srinivas, and K. Reddy, “A Decentralized Voting System Using Blockchain,” *Journal of Computational Analysis and Applications*, vol. 33, no. 5, pp. 567–575, 2024.

[5] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[6] G. Wood, “Ethereum: A Secure Decentralized Generalized Transaction Ledger,” Ethereum Yellow Paper, 2014.

[7] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[8] A. Kiayias and M. Yung, “The Vector-Ballot E-Voting Approach,” *Financial Cryptography and Data Security*, Springer, pp. 72–89, 2004.

[9] D. Chaum, “Secret-Ballot Receipts: True Voter-Verifiable Elections,” *IEEE Security & Privacy*, vol. 2, no. 1, pp. 38–47, 2004.

[10] J. Benaloh, “Simple Verifiable Elections,” *USENIX Security Symposium*, pp. 5–5, 2006.

[11] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," *arXiv preprint arXiv:1608.05187*, 2016.

[12] F. Hao, P. Y. A. Ryan, and P. Zielinski, "Anonymous Voting by Two-Round Public Discussion," *IET Information Security*, vol. 4, no. 2, pp. 62–67, 2010.

[13] N. Kshetri, "Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy," *Telecommunications Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[14] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2015.

[15] A. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," *IEEE Security and Privacy Workshops*, pp. 180–184, 2015.