



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secure and Transparent E-Voting System with Blockchain

Omkar Prajapati

Department of Data Engineering
Universal College of Engineering, Vasai,
Mumbai

Ravindra Sonavane

Department of Data Engineering
Universal College of Engineering, Vasai,
Mumbai

Aditya Singh Thakur

Department of Data Engineering
Universal College of Engineering, Vasai,
Mumbai

Akash Patil

Department of Data Engineering
Universal College of Engineering,
Vasai, Mumbai

Devansh Patil

Department of Data Engineering
Universal College of Engineering,
Vasai, Mumbai

Abstract — Ensuring transparency and reliability in electoral processes is essential for maintaining public trust in democratic systems. Conventional voting methods, including paper-based ballots and electronic voting machines, have raised concerns regarding security, transparency, and potential manipulation of results. This study proposes a blockchain-enabled electronic voting system designed to improve the integrity and auditability of digital elections. The system leverages Ethereum smart contracts to securely record votes on a decentralized ledger, ensuring that once a vote is submitted it cannot be modified or removed. Voter authentication is carried out through MetaMask wallet verification, which supports the enforcement of a one-voter–one-vote policy while preserving user anonymity. The architecture combines a web-based voting interface with blockchain-based smart contracts to manage vote submission and storage in an immutable ledger. Experimental implementation demonstrates that the proposed approach enhances transparency, reduces the possibility of vote tampering, and enables verifiable election results. The system can serve as a practical framework for conducting secure digital elections in educational institutions, organizational environments, and other controlled voting scenarios.

Keywords—Blockchain, Electronic Voting, Smart Contracts, Ethereum, MetaMask.

I. INTRODUCTION

Voting is a fundamental component of democratic governance, enabling citizens to participate in the selection of representatives and influence public decision-making. Traditionally, elections have been conducted using paper ballots or electronic voting machines (EVMs). Although these methods have been widely adopted, they still face challenges such as limited transparency, potential manipulation, and delays in vote counting. In many cases, voters must rely on centralized authorities to ensure the integrity of the election process, which can raise concerns regarding trust and security in the electoral system [6].

Electronic voting systems were introduced to improve the efficiency of election management and accelerate vote counting. However, most existing e-voting platforms rely on centralized databases that may be vulnerable to cyber-attacks, unauthorized access, or data manipulation. These limitations have encouraged researchers to explore decentralized technologies capable of enhancing election security and transparency. Blockchain technology has

emerged as a promising solution because of its decentralized architecture and immutable data storage capabilities [2].

Blockchain operates as a distributed ledger where transactions are verified and recorded across multiple network nodes. Once a transaction is confirmed and added to the blockchain, it becomes extremely difficult to modify or delete. This property makes blockchain suitable for applications that require high levels of transparency, integrity, and security, such as electronic voting systems. By storing votes as blockchain transactions, election records can become tamper-resistant while allowing independent verification of voting results [6].

Recent studies have also demonstrated that combining blockchain with cryptographic techniques and smart contracts can further enhance the reliability of voting systems. Cryptographic methods ensure voter privacy, while smart contracts automate election procedures such as vote validation and result calculation. These technologies collectively contribute to creating a transparent and secure digital voting infrastructure [4].

II. REVIEW OF LITERATURE

Electronic voting systems have been developed to improve the efficiency and accessibility of elections while reducing the time required for vote counting and result declaration. Traditional voting methods rely on paper ballots or electronic voting machines, which often require centralized control and manual verification procedures. Although these systems provide a structured mechanism for conducting elections, they can still suffer from issues such as limited transparency, security vulnerabilities, and the risk of unauthorized

manipulation. As digital technologies continue to evolve, researchers have increasingly explored secure electronic voting systems that can enhance election integrity while maintaining voter privacy.

Blockchain technology has emerged as a promising solution for addressing many of the security and transparency challenges associated with electronic voting systems. Blockchain functions as a distributed ledger that stores transactions across multiple nodes in a network, ensuring that the recorded data cannot be altered without consensus among participants. Because of its decentralized nature, blockchain eliminates the reliance on a single authority to manage election data and provides a tamper-resistant mechanism for recording votes. Several researchers have suggested that integrating blockchain with voting systems can enhance transparency, prevent vote manipulation, and enable independent verification of election results [6].

Recent studies have investigated the architectural frameworks of blockchain-based voting systems and their potential advantages over traditional voting infrastructures. A comprehensive survey of blockchain voting technologies highlights how distributed ledger systems can strengthen election reliability by ensuring that voting records remain immutable and publicly verifiable while maintaining voter confidentiality [5]. These studies also emphasize that blockchain voting platforms often incorporate smart contracts to automate vote validation and result calculation processes, thereby reducing the need for human intervention in critical election procedures.

Another important area of research focuses on analyzing the overall development and implementation of blockchain-enabled voting systems. Several systematic reviews have examined existing blockchain voting frameworks and compared their design principles, security mechanisms, and scalability characteristics. These analyses reveal that blockchain voting systems often employ cryptographic techniques such as digital signatures, hashing algorithms, and consensus protocols to guarantee secure vote recording and transparent result verification [3]. Such mechanisms ensure that once a vote has been submitted and validated within the blockchain network, it cannot be altered or removed without detection.

In addition to architectural improvements, researchers have also proposed advanced cryptographic methods to enhance privacy and security in blockchain-based voting systems. For instance, recent research introduces a cryptographic framework that combines symmetric and asymmetric encryption techniques to protect voter anonymity while maintaining the transparency of election results. By utilizing encryption algorithms such as AES and RSA, voting data can be securely stored and processed within blockchain networks without exposing sensitive voter information [1]. This approach demonstrates how cryptographic techniques can complement blockchain infrastructures to achieve both privacy preservation and transparent verification of votes.

Smart contracts have also been widely studied as an effective mechanism for implementing decentralized voting systems. Smart contracts allow predefined rules and conditions to be automatically executed within blockchain networks, making them suitable for managing voting processes. A notable example is the FASTEN protocol, which utilizes blockchain smart contracts to create a distributed voting system that ensures voter anonymity, vote immutability, and prevention of duplicate voting attempts [4]. By distributing trust across multiple network participants instead of relying on centralized authorities, such systems aim to improve fairness and reliability in digital elections.

Several surveys further highlight the growing interest in blockchain-based voting systems across academic research

and government initiatives. Researchers analyzing the evolution of blockchain voting technologies note that decentralized voting platforms have the potential to improve election transparency and voter confidence by enabling secure digital participation in electoral processes [2]. These studies also discuss the increasing adoption of blockchain voting solutions in various pilot projects around the world, indicating that blockchain technology may play an important role in shaping future election infrastructures.

Despite these promising developments, blockchain-based voting systems still face a number of challenges that must be addressed before they can be widely deployed in national-scale elections. Issues such as transaction scalability, network performance, and voter anonymity remain important research topics. Large-scale elections may generate millions of voting transactions within a short period of time, which requires efficient blockchain architectures capable of processing high volumes of data without compromising security or transparency. Furthermore, ensuring that voter identities remain confidential while maintaining verifiable election results continues to be an ongoing challenge in the design of blockchain voting systems.

Overall, existing research indicates that blockchain technology offers a strong foundation for developing secure and transparent electronic voting systems. By combining decentralized ledger architectures, cryptographic security mechanisms, and smart contract automation, blockchain-based voting platforms can potentially address many of the limitations found in traditional election systems. Continued research in this field is expected to further improve the scalability, security, and practical implementation of blockchain voting solutions, enabling more reliable and trustworthy digital election systems in the future.

Project Scope —

The scope of this project is to design and develop a secure and transparent electronic voting system using blockchain technology. The proposed system focuses on providing a decentralized platform where votes can be securely recorded and verified without relying on a centralized authority. By leveraging blockchain's distributed ledger architecture, the system ensures that once a vote is recorded, it cannot be altered or removed, thereby improving the integrity of the voting process.

The project aims to demonstrate how blockchain can enhance transparency and trust in digital elections by storing voting transactions in an immutable ledger. Each vote is treated as a blockchain transaction and is validated through smart contracts to prevent duplicate voting and unauthorized access. This mechanism ensures that every eligible voter can cast only one vote while maintaining the confidentiality of voter identity.

Another important aspect of the project is the use of cryptographic techniques to protect voting data. Encryption mechanisms are applied to ensure that voter choices remain confidential while the overall voting results remain transparent and verifiable. Additionally, the system provides a user-friendly interface that allows voters to participate in the election process easily.

The implementation of this system is primarily intended for academic institutions, organizations, and small-scale elections where secure digital voting is required. While the current prototype demonstrates the feasibility of blockchain-based voting systems, further improvements such as large-scale deployment, enhanced voter authentication, and improved scalability can be explored in future work.

Overall, the project focuses on developing a blockchain-based voting platform that improves security, transparency, and reliability compared to traditional electronic voting systems.

III. PROPOSED SYSTEM

The proposed system introduces a secure and transparent electronic voting platform built on blockchain technology. The primary goal of the system is to eliminate common vulnerabilities present in traditional voting mechanisms by leveraging decentralization, cryptographic security, and immutable data storage. The system is implemented as a decentralized application (DApp) that interacts with the Ethereum blockchain through smart contracts.

A. Voter Registration

The voting process begins with voter registration. Users register themselves through a web-based interface by providing necessary credentials such as their identification details. Once the registration is completed, the user connects their digital wallet through MetaMask. This wallet connection acts as a secure authentication mechanism, allowing the system to uniquely identify each voter.

B. Authentication and Login

Authentication in the proposed system is handled through wallet-based verification instead of traditional username–password systems. When a voter logs into the platform, MetaMask verifies the wallet address associated with the user. This method enhances security by preventing unauthorized access and ensuring that only verified users can participate in the election process.

C. Vote Casting

After successful authentication, voters can access the voting dashboard where the list of candidates is displayed. The voter selects their preferred candidate and submits the vote through the voting interface. The voting transaction is then executed through an Ethereum smart contract, which records the vote securely on the blockchain network.

The system enforces a strict one-account–one-vote policy by verifying whether a wallet address has already participated in the election. If a voter attempts to vote multiple times, the smart contract rejects the transaction automatically.

D. Vote Recording on Blockchain

Each vote is recorded as a blockchain transaction and stored on a distributed ledger. Blockchain technology ensures that once a vote is recorded, it cannot be altered or deleted. The decentralized nature of blockchain eliminates reliance on a central authority and allows transparent verification of voting transactions.

E. Result Display

The system provides real-time vote counting by reading transaction data directly from the smart contract. Election results are displayed through the web interface once the voting period ends. Since all votes are recorded on the blockchain, the results remain transparent and verifiable by all participants.

IV. SYSTEM ARCHITECTURE AND METHODOLOGY

The proposed blockchain-based electronic voting system is designed as a decentralized application that enables secure and transparent voting operations. The architecture integrates user interaction modules with blockchain infrastructure to ensure that voting data is stored in a tamper-resistant and verifiable manner. Instead of relying on a centralized database, all vote transactions are recorded on a blockchain ledger, which enhances transparency, security, and reliability in the election process.

A. SYSTEM ARCHITECTURE

The architecture of the proposed system consists of several functional modules that manage user interaction, voting activities, and administrative operations.

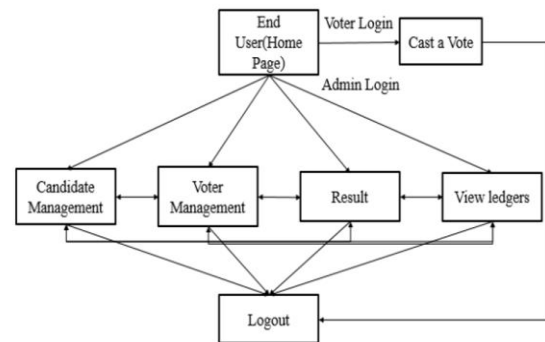


Fig. 1. System architecture of the proposed voting system

1. User/Home Page

The User/Home Page acts as the entry point of the system. It provides a simple interface where users can access the voting platform. From this page, users can choose whether to log in as a voter or as an administrator. This module ensures easy navigation and provides the starting point for the voting workflow.

2. Voter Login

The voter login module allows registered voters to authenticate themselves before participating in the election. Only authorized voters are allowed to access the voting interface. After successful authentication, voters are redirected to the voting dashboard where they can view candidate information and participate in the voting process.

3. Admin Login

The admin login module is designed for election administrators who manage and monitor the voting process. Administrators have access to system management features such as candidate registration, voter management, and result monitoring. This module ensures that only authorized personnel can perform administrative operations.

4. Candidate Management

The candidate management module allows administrators to add, update, or remove candidate information before the election begins. This component stores candidate details and ensures that voters can view accurate candidate data during the voting process.

5. Voter Management

The voter management module maintains the list of eligible voters. It allows administrators to register voters and verify their eligibility before the voting process starts. This component helps prevent unauthorized users from participating in the election.

6. Cast Vote

The cast vote module allows authenticated voters to select their preferred candidate and submit their vote. Once a vote is cast, it is recorded as a transaction on the blockchain network. The decentralized nature of blockchain ensures that each vote is securely stored and cannot be modified.

7. View Ledger

The view ledger module provides transparency by allowing users or administrators to inspect the blockchain ledger. Through this module, voting transactions can be verified to ensure that votes have been recorded correctly and that the election process remains transparent.

8. Result Module

The result module calculates and displays the final election results based on the votes stored on the blockchain. Since all voting transactions are recorded on the distributed ledger, the results can be verified easily without the risk of data manipulation.

9. Logout

The logout module enables users to safely exit the system once their session is completed. This ensures that unauthorized access is prevented after the user finishes interacting with the voting platform.

B. METHODOLOGY

The methodology of the proposed blockchain-based voting system describes the operational workflow followed during the election process. The system follows a sequence of steps that ensure secure voter authentication, vote recording, and transparent result generation using blockchain technology.

1. User Access and System Entry

The process begins when a user accesses the voting platform through the home page. The system provides two access options: voter login and administrator login. This separation ensures that voters and administrators can only access the functions assigned to their roles.

2. Voter Authentication

Before participating in the election, voters must authenticate themselves through the voter login module. The system verifies voter credentials and ensures that only registered users can access the voting interface. This step prevents unauthorized access and maintains the integrity of the election process.

3. Candidate and Voter Management

The administrator is responsible for managing election data before the voting process begins. Through the candidate management module, the administrator registers candidates who will participate in the election. Similarly, the voter management module is used to maintain the list of eligible voters. These modules ensure that only valid candidates and voters are included in the system.

4. Vote Casting Process

After successful authentication, voters can access the voting interface where the list of candidates is displayed. The voter selects a candidate and submits their vote through the system. Once submitted, the vote is processed and converted into a blockchain transaction to ensure secure storage.

5. Recording Votes on the Blockchain

Each vote is stored on the blockchain ledger as a transaction. Blockchain technology ensures that the stored voting data remains immutable, meaning that once a vote is recorded, it cannot be modified or deleted. This feature enhances transparency and prevents vote manipulation.

6. Ledger Verification

The system provides a ledger viewing feature that allows administrators to verify the recorded voting transactions. By accessing the blockchain ledger, election data can be checked to ensure that all votes have been securely recorded and that no unauthorized changes have occurred.

7. Result Generation

Once the voting process is completed, the system calculates the final election results based on the votes stored on the blockchain. Because all votes are securely recorded on the distributed ledger, the results can be generated accurately and transparently.

8. Secure Logout

After completing their activities, users exit the system through the logout module. This step terminates the session securely and prevents unauthorized access to the voting platform.

V. RESULTS

The proposed blockchain-based electronic voting system was implemented and tested in a simulated election environment. The system integrates a web-based voting interface with Ethereum smart contracts to ensure secure vote recording and transparent result verification. The experimental results demonstrate that the system successfully supports voter authentication, candidate management, vote casting, and real-time result generation through blockchain transactions.

1. MetaMask Authentication

Before accessing the voting system, users must connect their MetaMask wallet to the decentralized application. MetaMask acts as the authentication mechanism that verifies the user's blockchain address and allows secure interaction with the Ethereum network.

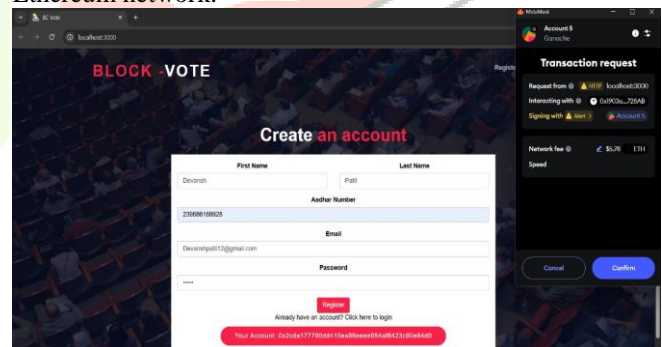


Fig.2 MetaMask wallet authentication interface

The interface shown in Fig. 2 demonstrates how the system requests permission from the user's MetaMask wallet to establish a secure blockchain connection. Once the wallet is connected, the user can interact with the voting application and perform transactions such as registration or vote casting. This authentication method eliminates the need for traditional username-password systems and improves system security.

2. Admin Dashboard

After successful authentication, the administrator can access the admin dashboard to configure the election process.

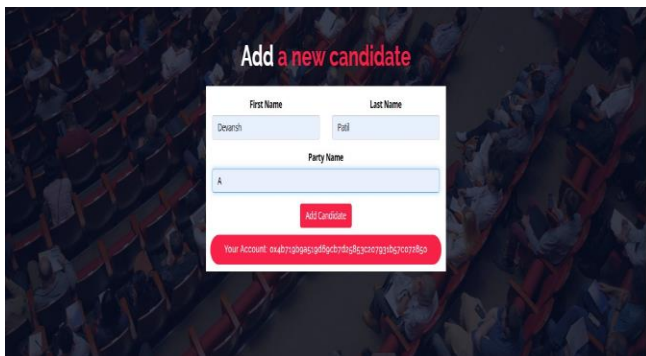


Fig. 3. Administrator dashboard

As illustrated in Fig. 3, the admin dashboard allows administrators to add candidates, manage election settings, and monitor system activities. Through this interface, the election process can be initialized by registering candidates and preparing the system for voter participation. The use of blockchain ensures that all administrative actions related to election configuration are securely recorded.

3. Voter Registration Interface

Before participating in the election, users must register themselves in the system.

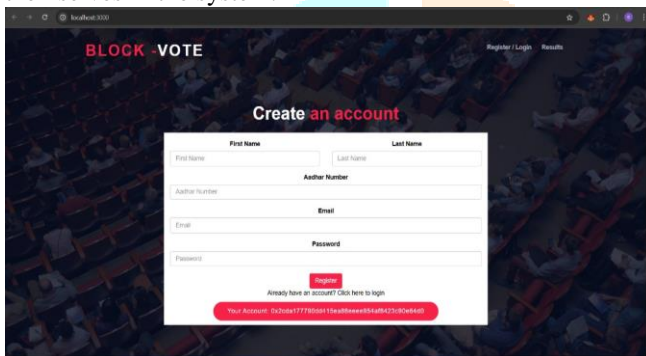


Fig. 4. Voter Registration Interface

The registration interface shown in Fig. 4 allows users to create an account by providing required details. Once registered, voters can access the voting platform and participate in the election process. The system verifies voter eligibility and ensures that each registered user can vote only once.

4. Voting Interface

Once registration and authentication are completed, voters are allowed to cast their votes through the voting interface.

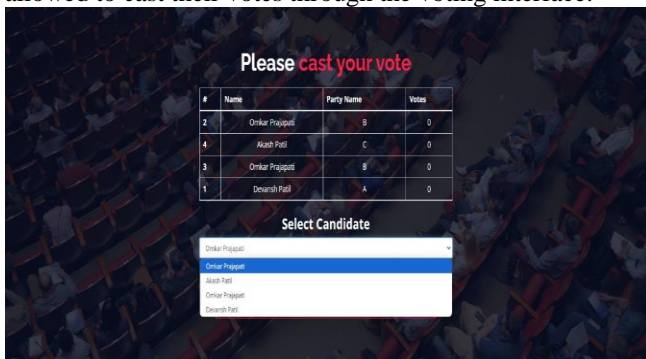


Fig. 5. Candidate selection interface

Fig. 5 illustrates the voting interface where voters can select their preferred candidate and submit their vote. After the vote is cast, the transaction is recorded on the blockchain network through a smart contract. This ensures that the vote cannot be altered or deleted, maintaining the integrity of the election process.

5. Result Interface

After the voting process is completed, the system displays the election results.



Fig. 6. Election result dashboard

The result interface shown in Fig. 6 presents the final vote counts for each candidate. Since all votes are stored on the blockchain ledger, the results can be verified transparently. The real-time result display improves trust in the voting process and eliminates the possibility of manual manipulation.

Result Analysis

The experimental implementation confirms that the blockchain-based voting system provides several advantages over traditional voting mechanisms. The use of smart contracts ensures that voting rules such as the one-person-one-vote policy are automatically enforced. Additionally, the decentralized nature of blockchain guarantees that recorded votes remain immutable and publicly verifiable. The system successfully demonstrates secure authentication, transparent vote recording, and reliable result generation, making it suitable for small-scale organizational or institutional elections.

CONCLUSION

This research presented the design and implementation of a blockchain-based electronic voting system aimed at improving the security, transparency, and reliability of digital elections. Traditional voting methods, including paper ballots and electronic voting machines, often face challenges related to trust, transparency, and susceptibility to manipulation. To address these issues, the proposed system integrates blockchain technology with smart contracts to create a decentralized voting platform.

The implemented system demonstrates how blockchain can be used to securely record votes as immutable transactions on a distributed ledger. Through the integration of Ethereum smart contracts, MetaMask authentication, and a web-based voting interface, the platform ensures that each voter can cast only one vote while maintaining voter anonymity. The system also provides transparent result verification, allowing election outcomes to be viewed and validated directly from the blockchain ledger.

The experimental results confirm that the proposed system successfully supports key election operations such as voter registration, candidate management, vote casting, and result generation. The decentralized nature of blockchain enhances trust in the voting process by preventing vote tampering and ensuring the integrity of election data.

Overall, the developed blockchain-based voting platform demonstrates the potential of decentralized technologies in modernizing electoral systems. The proposed model can be applied to small-scale elections such as academic institutions, organizations, or local governance structures. With further improvements in scalability, privacy mechanisms, and regulatory integration, blockchain-based voting systems could

become a viable solution for secure and transparent digital elections in the future.

REFERENCES

- [1] M. Galal, E. A. E. Reheem, and S. Guirguis, "Enhancing Privacy and Transparency in Electronic Voting: A Blockchain-Based Cryptographic Framework," *Journal of Cloud Computing*, 2026.
- [2] M. V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," *IEEE Access*, vol. 11, 2023.
- [3] 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, 2022.
- [4] S. Damle, S. Gujar, and M. Moti, "FASTEN: Fair and Secure Distributed Voting Using Smart Contracts," 2021.
- [5] H. O. Ohize et al., "Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges," *Cluster Computing*, 2024.
- [6] I. Singh et al., "Enhancing Security and Transparency in Online Voting through Blockchain Decentralization," *SN Computer Science*, 2024.
- [7] K. Zhang, H. Li, and Y. Wang, "A Blockchain-Based Electronic Voting System for Transparent and Secure Elections," *IEEE Access*, 2023.
- [8] A. Kiayias and M. Yung, "Self-Tallying Elections and Blockchain Voting," *International Journal of Information Security*, 2020.
- [9] P. McCorry, S. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," *Financial Cryptography and Data Security*, 2017.
- [10] R. Hanifatunnisa and B. Rahardjo, "Blockchain Based E-Voting Recording System Design," *IEEE International Conference on Telecommunication Systems*, 2017.

