International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Design and Implementation of a Secure and Transparent Decentralized Voting System using Blockchain Technology

Bishwa Prakash Prajapati
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
Bishwaprakash900@gmail.com

Samim Khan
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
Samim.khan021@gmail.com

Mikhail Janli Purba
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
Janli.purba@gmail.com

Kamal Singh
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
Kamalsinghbs347@gmail.com

Anant Pathak
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
Anantpathak560@gmail.com

Dr. Ajay Kumar Singh
Department of Computer Science and Engineering
Jain Deemed-to-be University
Bengaluru, India
Ajay.k.singh@jainuniversity.ac.in

Abstract*—The integrity and transparency of voting systems are fundamental to the democratic process; however, traditional voting mechanisms often encounter issues such as fraud, manipulation, limited transparency, and centralized control. To address these challenges, this research proposes a decentralized voting system utilizing blockchain technology. The system leverages the Ethereum blockchain, smart contracts developed in Solidity, and a React.js-based frontend integrated with Web3.js and MetaMask to ensure secure voter authentication, transparent vote casting, and immutable vote recording. Voter and candidate registrations are managed through decentralized smart contracts, and all transactions are permanently stored on the blockchain, providing public verifiability while preserving voter anonymity. Development and testing were conducted in a simulated environment using Ganache and the Truffle Suite, allowing for extensive validation of system functionalities. Experimental results demonstrate enhanced security, real-time result computation, prevention of double voting, and elimination of any single point of failure. This decentralized architecture significantly improves trust, transparency, and security in electoral processes, offering a scalable and reliable model for the future of electronic voting systems.

***Index Terms*— Blockchain, Decentralized Voting, Ethereum, Smart Contracts, Solidity, Web3.js, MetaMask, Ganache, Truffle Framework, E-voting Systems.**

I. INTRODUCTION

Millions Voting is one of the most important aspect of any democratic society as it allows citizens to actively take part in shaping government policies and determining governance through an election [1]. Yet, both paper and electronic voting systems have always struggled with issues relating to security, transparency, access for people with disabilities, and trust from the public. Other better systems facing voter fraud, election security breaches, results being overridden, prone to failures, no adequate verification, audit routes having centralized systems are problems observed in today's state of the art voting systems. [2], [3]

Recently, many systemic problems have surfaced today's world and blockchain technology have proven to be a one stop remarkable solution. The blockchain provides a transparent ledger which is unchangeable and decentralized so that once any piece of information is documented, it requires a mutual agreement for it to be changed. [4] The disposition makes blockchain a foremost choice regarding repairing installation of modernized voting approaches that provides safety, public confidence and ensures accuracy of elections results protecting them from manipulations.

The current research attempts with deploying decentralized voting utilizing block chain technology along with smart contracts, web interfaces and user friendly frontends. Authentication on the MetaMask wallets gives access via React.js with Web3.js forming new frontiers on Ethereum blockchain smart contracts which establishes safe access enabling registration, verifiable voting, serving information access during elections, counted votes and ledger documents securing unified modification. The system architecture was implemented and tested using Ganache, a personal blockchain for rapid development, and Truffle Suite for contract deployment and migration.

Voting systems' honesty and openness play a key role in democracy. Yet old-school voting often runs into problems like cheating meddling, lack of openness, and too much central control.[5] To fix these issues, this study suggests a spread-out voting system using blockchain tech. The system taps into the Ethereum blockchain smart contracts written in Solidity, and a React.js front-end that works with Web3.js and MetaMask. This setup makes sure voters can prove who they are , votes are cast , and votes are recorded in a way that can't be changed. Smart contracts that aren't controlled handle signing up voters and candidates. All dealings are kept on the blockchain for good letting anyone check them while keeping voters' names secret. [6] The team built and tested the system in a mock setting using Ganache and the Truffle Suite, which let them check all parts of the system . Tests show the system boosts safety, figures out results right away, stops people from voting twice, and gets rid of any weak points that could bring down the whole system. This spread-out setup boosts trust, openness, and safety in voting. It offers a model for future e-voting systems that can grow and won't let you down.

II. RELATED WORKS

Preserving the security, transparency, and trust of voting systems has been an issue of concern for many decades. Voting with paper documents can be audited, however, they lack in practicality because of issues like logistical problems, ballot stuffing, and tampering.[7] Internet-based voting systems and voting machines are much more effective when it comes to efficiency, but create several new issues, such as the software susceptibility features, transparency issues, loss of anonymity for voters, and the most important central control. Technologists and researchers are motivated to look for alternatives after facing these challenges, in attempts to strengthen the integrity and trust of the democratic process.

The latest trend of blockchain technology came into existence with Bitcoin, thanks to Satoshi Nakamoto in 2008. [8], [5] It is the first decentralized approach that showcases immutability, transparency, and trust on various levels. Because of these distinctive benefits, there has been an increased interest in applying blockchain with electoral systems to solve the shortcomings of traditional methods.

A primary FollowMyVote sponsored a voting platform that was based on blockchain technology where votes are signed cryptographically and can be verified by voters which are recorded publicly.[9], [3] Although this platform provided impressive transparency, it suffered a lot in terms of usability ensuring complete voter anonymity and ease of access for non-technical users, seeing that blockchain transactions cannot be hidden.

During several elections in the United States, a mobile voting app known as Voatz which includes blockchain and biometric features was put through pilot testing. Voatz demonstrated the practical potential of mobile blockchain voting; however, it attracted criticism from cybersecurity researchers for security vulnerabilities, such as susceptibility to server compromise and lack of end-to-end verifiability, as highlighted by a 2020 MIT study. [10]These shortcomings underscored the difficulties in balancing security, privacy, and accessibility within blockchain voting implementations.

Academic work has thoroughly investigated the use of blockchain in elections. As an example, Hardwick et al. (2018) in their paper "E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy" suggested utilizing smart contracts to mechanize election processes. [11], [12] Their paper emphasized the importance of privacy-preserving methodologies along with publicly transparent recording but recognized possible scalability concerns, especially when handling millions of voters on public blockchains such as Ethereum.

Although these beneficial contributions exist, shared gaps prevail among current research studies and projects:

- Scalability: High transaction fees and delays on public blockchains can impede real-time voting operations, particularly during high voter turnout.
- Voter Privacy: Balancing transparency with absolute voter confidentiality continues to pose technical and ethical challenges.
- Usability: Many blockchain voting systems are complex, making adoption difficult for non-technical users.
- Security Risks: Wallet integration vulnerabilities and flaws in smart contract coding can introduce new attack vectors [13].

A. Comparison with Our Work

Our suggested decentralized voting system straight away resolves the present issues by coming up with an applicable prototype utilizing Ethereum smart contracts for electoral administration, MetaMask wallet verification for safe voter identity, and a React.js-based user interface for ease of use. Our system provides:

- Enhanced usability: A streamlined interface allows users to easily register, cast votes, and view results without deep technical knowledge.
- Transparency with privacy: Voter authentication is handled securely through wallet addresses without disclosing any personal information, preserving anonymity while maintaining auditability.
- Efficient performance in simulated environments: Through the use of Ganache for local blockchain simulation and Truffle Suite for deployment, the system successfully handled multiple voter transactions without failure, laying groundwork for scaling strategies in future real-world applications.
- Immediate vote finality and immutability: Each cast vote is permanently recorded on the blockchain, eliminating the risk of retroactive vote alteration or deletion.

While scalability to national elections is still an open area of research — as with most blockchain-based voting platforms — our solution draws from the experience gained in previous projects such as FollowMyVote, Voatz, and academic proofs-of-concept to offer a refined framework more suited to real-world adoption.

By ensuring proper integration of decentralized technology with user-focused design, this study adds to the collective worldwide endeavor to develop more secure, transparent, and accessible ballot systems based on blockchain technology.

III. Methodology

The creation of the Decentralized Voting System on blockchain technology takes a structured approach to the process of designing a secure, transparent, tamper-proof, and user-friendly electronic voting platform. The structured approach was split across various phases of requirement analysis, system design, smart contract writing, blockchain simulation, frontend design, integration of wallet, deployment, testing, and assessment.

A. Requirement Analysis

The project began with a comprehensive requirement analysis to identify the critical features necessary for a reliable voting system. Essential requirements included:

- Voter registration and authentication.
- Candidate registration and management.
- Secure vote casting while preventing double voting.
- Real-time result computation.
- Transparency without compromising voter anonymity.

B. System Architecture Design

Following After evaluating blockchain's strengths — decentralization, immutability, and security — Ethereum was chosen for its robust ecosystem, developer tools, and security. Truffle and Ganache are used for smart contract development and testing.

Table. 1 The decentralized voting system has four layers: The Smart Contract Layer, built with Solidity and Truffle, handles voter enrollment and vote counting. The Blockchain Network Layer, based on Ethereum and run via Ganache, ensures tamper-proof, transparent transactions.[15], [9] The Frontend Application Layer, developed with React.js and Web3.js, provides a user-friendly interface for vote submission. The Wallet and Provider Layer uses MetaMask for secure authentication and transaction signing. This architecture ensures security, scalability, and easy future upgrades.

Layer	Technology Stack	Core Functionality
Smart Contract Layer	Solidity, Truffle	Core backend logic for managing candidates, voters, voting, and result computation.
Blockchain Network Layer	Ethereum Blockchain (Ganache for local simulation)	Distributed ledger for securely recording all voting transactions and smart contract states.
Frontend Application Layer	React.js, Web3.js, MetaMask	User interface for voters to interact with the blockchain: register, cast votes, and view results
Wallet and Provider Layer	MetaMask	Manages user authentication and transaction signing during voting.

Table 1: proposed System Architecture

C. Smart Contract Development

The voting system operates on smart contracts which are written in Solidity. [15], [12] Within Candidate Management a structure alongside a mapping containing candidate's data is responsible for effortless accessibility and retrieval pertaining to a list of candidates. For Voter Management, there were systems put in place for capturing the activity of voters and restricting the possibility of multiple voting to maintain trust within the elections. Each vote is authenticated and stored in a manner that cannot be altered and hence secured in the respective vote() function encapsulated under Voting Functionality. Vote tallying is completed in a reliable manner with no hidden agendas, executed through the getResults() function which always provides the expected outcome. Migration scripts (1_initial_migration.js and 2_deploy_contracts.js) were also developed to permit quick updates and easy deployment of these smart contracts on the Ethereum blockchain or facilitate any subsequent modification which would streamline the process already outlined.

D. Blockchain Simulation

To facilitate flexible and efficient development, a local blockchain environment was mimicked using Ganache CLI. This simulation allowed for testing in a controlled environment without the need for real Ethereum transactions, making it cost-effective and rapid. Ganache provided multiple pre-funded Ethereum accounts, which were used to imitate different responsibilities, such as administrators and voters. This approach enabled the team to perform tests without any risk of paying gas bills, while also facilitating rapid iterations and debugging during the development process. The usage of Ganache ensured a flawless testing environment that replicated the real blockchain experience. Fig. 1 shows a private Ethereum (ETH) account generated through Ganache for local blockchain development.

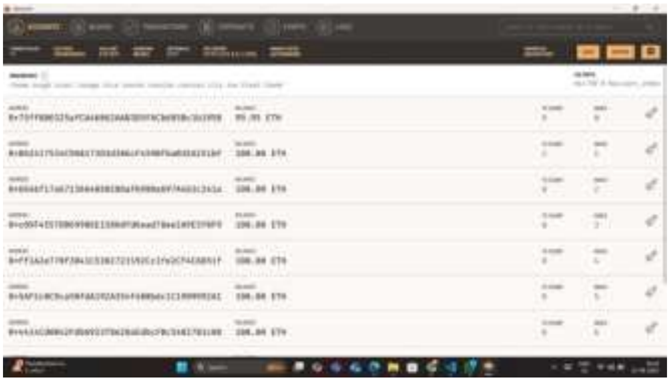

Fig. 1. Private ETH account created using Ganache.

E. Frontend Development

The frontend of the decentralized voting application was developed via the React.js framework, allowing for a clean, responsive user interface. Key functions of the application consists of connecting users MetaMask wallets, presenting a list of registered candidates, and enabling voters to cast a secure vote. Fig. 2 presents the admin page interface of the proposed system. Additionally, the frontend displayed live election results to enhance transparency and engage the community. Therefore, connection to Web 3.0 was paramount for the frontend to seamlessly communicate with deployed smart contracts for blockchain interaction via the Ethereum blockchain. React.js was also helpful as it kept the application user-friendly while being responsive to a myriad of devices and screen sizes.

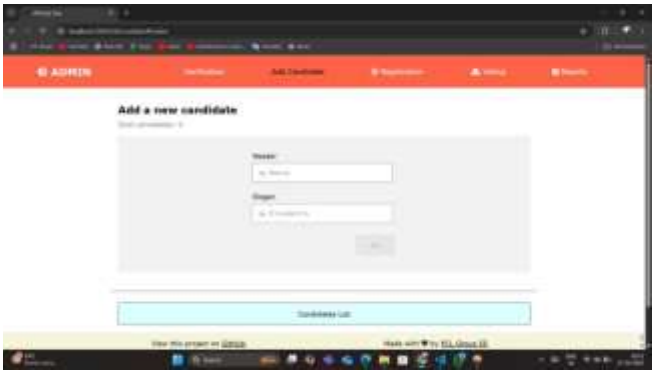

Fig. 2. Admin page of the proposed system.

F. Wallet Integration and Authentication

Metamask integration was important to ensure secure user authentication and transaction signature. A customized tool script, Getweb3.js, was designed to handle significant functionalities: Finding out if metamask was installed, establishing a connection with the atherium wallet and creating a web 3 examples for communication between the front and smart contracts. The user authentication was based on the voter's atherium address, and ensured that only registered and qualified voters can participate in the election. Metamaska provided the necessary protection by managing private keys and signing the transaction at the local level, which made the voting process safe and user -friendly. Fig. 3 illustrates the Metamask integration process in the system.

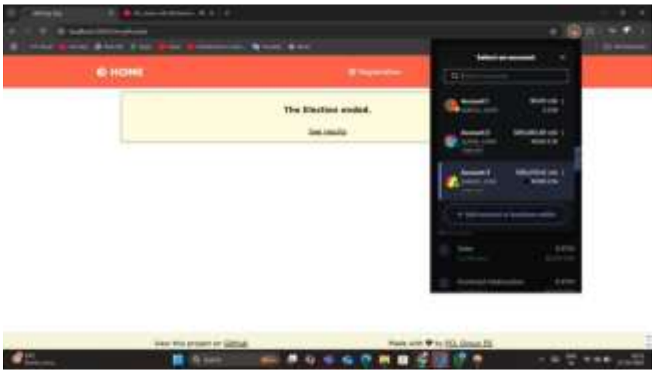

Fig. 3. Metamask integration process.

G. Deployment and Testing

The Smart contracts were compiled and deployed on the Ganache blockchain using the Truffle CLI in order to establish a system the user could interact with and test. As outlined previously, we could verify the deployment procedure via the migration logs to confirm that each contract had been deployed. To accomplish the aim of this project, the system was subjected to extensive testing. In this case, testing involved simulated voting operations using multiple Ethereum accounts. Testing scenarios were conducted in order to confirm user eligibility was enforced correctly, that double voting was avoided, and that vote counts were accurate. The results were validated using Ganache logs as well as MetaMask transaction logs in order to confirm that the deployed system operated correctly under various scenarios.

H. Evaluation

The system was further evaluated against four criteria, following the implementation and testing phases: security, transparency, accuracy and usability. The system's security was assessed by verifying that votes would be stored securely and immutably on the blockchain. Transparency was evaluated by accounting for the credibility of the records of votes, which can be publicly verified, but without compromising the anonymity of the voter. Accuracy was verified via testing to make certain the system returned the correct vote counts, and usability was verified by seeing that the system was user-friendly and provided a satisfactory user experience. The system demonstrated it would defend against realistic adversarial threats, provide real time results, and deliver a user-centric interface to achieve the voting experience.

IV Results and Discussion

proposed decentralized voting system has been successfully developed, deployed, and tested in a simulated environment using the Ethereum blockchain and Ganache. This section summarizes the key results obtained when testing the system and discusses how eff ectively the system achieved the project objectives. The system deployment involved a local deployment of the smart contracts onto a Ganache local blockchain network, with the Truffle Suite used to compile and deploy the smart contracts. The front-end application was built using React.js and connected with the deployed smart contract via Web3.js and MetaMask allowing for secure active interaction between users and the blockchain network.

The system simulated several real-world scenarios to provide the system core functionalities. During voter registration, each user was authenticated via MetaMask and their identity verified with a unique Ethereum address. Candidate registration was successfully completed by administrative users which allowed administrative users to register candidates by directly interacting with the smart contract which manages candidate registration. Votes were cast securely and voters were restricted to only being able to cast a single vote by the smart contract that will not allow double voting. In terms of vote count, votes were counted in real time and displayed as soon as the vote was cast. Fig. 4 The visual display of the vote counted was a standard number derived from the direct data pulled from the blockchain.

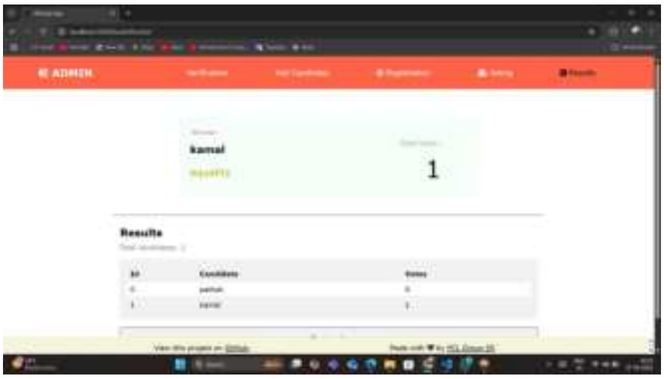

Fig.4. final result of election

Additionally, immutable vote recording was confirmed using transaction logs on Ganache, where each transaction indicating a vote was permanently logged on the blockchain. This immutability assured that once a vote was cast, it could not be amended or removed, confirming the system's integrity and security.

Overall, the system met its objectives by proving secure voter authentication, transparent and real-time vote counting, prohibition of multiple voting attempts, and tamper-proof record preservation, all within a decentralized framework. Table II summarizes the key observations and their current status.

Test Scenario	Expected Result	Observed Outcome	Status
Voter Authentication via MetaMask	Successful	MetaMask connection established securely	✔
Candidate Registration	Candidates added correctly to smart contract	Candidates appeared on voting list	✔
Single Vote per User	Vote should be cast only once	Smart contract rejected duplicate votes	✔
Vote Count Accuracy	Correct vote tally expected	Real-time accurate tallying observed	✔
Transaction Immutability	Votes cannot be altered once cast	Verified on Ganache transaction log	✔
Result Declaration	Display after all votes cast	Results updated instantly on frontend	✔

Table 2: key Observations and status

V. Conclusion

The design and implementation of the Decentralized Voting System using blockchain technology illustrates the potential of decentralized platforms to transform traditionally centralized voting systems. By utilizing the Ethereum blockchain, smart contracts and a React.js-based frontend, the Decentralized Voting System addressed many of the limitations found in conventional voting systems, including exposure to fraud, lack of transparency and excessive reliance on centralised authorities.

The designed platform allowed for every vote to be maintained securely for future, immutable access on a blockchain ledger. This made the voting process tamper-proof, verifiable by anyone, and public. The Decentralized Voting System prevented double-voting with MetaMask integration and account-level authentication, allowing real-time elections results while also ensuring voter anonymity. While the voting system was in operation, the decentralized architecture was viewed as more favorable compared to a centralized model because of the inherent lack of a single point of failure and the ability to trust the overall voting process more.

Overall, this project demonstrated that blockchain technology could appreciably improve the security, transparency and efficiency involved with voting systems. Although what we have described was run into a simulated blockchain environment (Ganache), it opens the doors to testing on a real-world blockchain in the future, with further scalability, privacy improvements and compliance with standards. With more research and development, decentralized voting systems could be introduced as a legitimate option in future democratic practices, while ensuring that citizens feel trust and engagement within the process.

VI. References

[1] Al-Madani, Ali Mansour, et al. "Decentralized E-voting system based on Smart Contract by using Blockchain Technology." 2020 international conference on smart innovations in design, environment, management, planning and computing (ICSIDEMPC). IEEE, 2020.

[2] Patil, Harsha V., Kanchan G. Rathi, and Malati V. Tribhuwan. "A study on decentralized e-voting system using blockchain technology." Int. Res. J. Eng. Technol 5.11 (2018): 48-53.

[3] Garg, Kanika, et al. "A comparitive analysis on e-voting system using blockchain." 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). IEEE, 2019.

[4] Huang, Jun, et al. "The application of the blockchain technology in voting systems: A review." ACM Computing Surveys (CSUR) 54.3 (2021): 1-28.

[5] Hardwick, Freya Sheer, et al. "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy." 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). IEEE, 2018.

[6] Alvi, Syada Tasmia, et al. "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system." Journal of King Saud University-Computer and Information Sciences 34.9 (2022): 6855-6871.

[7] Patidar, Kriti, and Swapnil Jain. "Decentralized e-voting portal using blockchain." 2019 10th international conference on computing, communication and networking technologies (ICCCNT). IEEE, 2019.

[8] Indapwar, Aishwarya, Manoj Chandak, and Amit Jain. "E-voting system using blockchain technology." Int. J. of Advanced Trends in Computer Science and Engineering 9.3 (2020).

[9] Garg, Kanika, et al. "A comparitive analysis on e- voting system using blockchain." 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). IEEE, 2019. [10]A.

[11] Almeida, Ricardo Lopes, et al. "Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey." IEEE Access 11 (2023): 132389-132423.

[12] Barbereau, Tom, et al. "Decentralised finance's timocratic governance: The distribution and exercise of tokenised voting rights." Technology in Society 73 (2023): 102251.

[13] Jafar, Uzma, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. "Blockchain for electronic voting system—review and open research challenges." Sensors 21.17 (2021): 5874.

[14] Jangada, Atharva, et al. "De-centralized voting system using blockchain." 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS). IEEE, 2022.

[15] Patel, Devarsh, et al. "Decentralised Blockchain-Based Framework for Securing eVoting System." International Conference on Expert Clouds and Applications. Singapore: Springer Nature Singapore, 2022.