



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

Distributed Voting System by Using Blockchain Ethereum with Ganache

N. Likhith, R. Kavya, V. Krupakar, D. Koushik Reddy, Dr. G. Nanda Kishor Kumar

Department of Computer Science & Engineering Malla Reddy University, Hyderabad Maisammaguda, Kompally,
Hyderabad, India

ABSTRACT: Ensuring secure, transparent, and tamper-proof elections is a critical challenge in modern democracy. Traditional voting systems, including paper ballots and electronic voting machines (EVMs), suffer from issues such as voter fraud, vote tampering, high operational costs, and limited accessibility. This project introduces an "Online Voting System Using Blockchain Ethereum with Ganache," a decentralized and secure voting platform leveraging blockchain technology. The system records votes immutably on the Ethereum blockchain using smart contracts deployed via Ganache. To enhance security, it integrates face recognition authentication and email OTP verification, ensuring that only authorized voters can participate, eliminating impersonation and multiple voting. Decentralization prevents manipulation, making election results verifiable and tamper-proof. Developed using HTML, CSS, JavaScript, Bootstrap, Python, Django, Web3.js, and Solidity, the system offers a user-friendly interface for voters and administrators. The backend, built with Django, manages authentication, election operations, and blockchain interactions. Automated vote counting ensures instant, accurate, and transparent election results. Ganache facilitates smart contract testing before deployment on a live network. This system eliminates the vulnerabilities of traditional voting, providing a secure, efficient, and trustworthy alternative. By leveraging blockchain's decentralization and transparency, it sets a new standard for digital democracy, enhancing election integrity and voter confidence.

KEYWORDS: Blockchain, Ethereum, Ganache, Smart Contracts, Online Voting, Face Recognition, OTP Verification, Decentralization, Secure Elections.

I. INTRODUCTION

In the modern digital era, technological advancements have transformed various industries, yet the electoral process in many regions continues to rely on traditional methods that often prove inefficient and susceptible to fraud. Conventional voting systems, whether paper-based or electronic, face challenges such as manipulation, tampering, and security breaches, which can lead to disputes and a loss of trust in the democratic process. To address these issues, blockchain technology offers a decentralized, secure, and transparent solution for conducting elections.

The Online Voting System Using Blockchain Ethereum with Ganache is designed to enhance the voting process by integrating face recognition for voter authentication and email OTP validation to verify voter identity before casting a vote. The system employs Ethereum blockchain technology to store votes securely and immutably, ensuring that election results remain unaltered and verifiable. With the use of Ganache, a personal Ethereum blockchain, a controlled testing environment is provided for deploying and managing smart contracts that facilitate the voting process and result computation.

Developed using HTML, CSS, JavaScript, and Bootstrap for the front-end, the system delivers a responsive and user-friendly experience. The back-end, built on Python and Django, efficiently handles user authentication, election management, and vote recording. The blockchain integration ensures that every vote is transparently recorded, making the system highly resistant to fraud and guaranteeing the credibility of election outcomes. By eliminating the risks associated with traditional voting systems, this project provides a secure, efficient, and reliable alternative that can be adopted for various types of elections.

Traditional voting processes face several challenges that significantly affect the fairness and accuracy of elections. One of the most concerning issues is voter fraud, which includes unauthorized voting, impersonation, and multiple voting attempts by the same individual. Such fraudulent activities undermine the legitimacy of election results and lead

to a decline in public trust in the electoral process. Moreover, traditional voting methods lack transparency, making it difficult for voters to verify whether their votes have been counted accurately, further diminishing confidence in the system.

Another major concern is the security vulnerability of electronic voting systems, which rely on centralized databases and servers that are prone to cyberattacks, hacking, and unauthorized access. These threats can result in data breaches, vote manipulation, and other forms of electoral fraud, ultimately compromising the integrity of elections. Additionally, organizing elections through traditional methods is both time-consuming and costly, requiring significant resources for setting up polling stations, deploying election officials, and conducting manual vote counting. These inefficiencies make elections expensive, slow, and prone to human errors.

Limited accessibility to polling stations also hinders voter participation. Individuals with disabilities, those living in remote areas, and people with time constraints often find it difficult to reach polling locations, resulting in lower voter turnout. Consequently, election results may not truly reflect the will of the people. Implementing an online voting system that leverages blockchain technology ensures a secure, transparent, and efficient electoral process, enabling voters to participate remotely while guaranteeing that every vote is accurately counted and securely stored.

This project aims to develop a secure and transparent online voting system that utilizes the Ethereum blockchain and Ganache to ensure that the electoral process remains tamper-proof, verifiable, and resistant to fraud. By incorporating blockchain technology, the system eliminates the risks associated with traditional voting methods while enhancing security, trust, and efficiency. The goal is to create a decentralized voting platform where votes are securely recorded and cannot be altered, ensuring the integrity of election results.

A key objective of the system is to implement face recognition and email OTP verification as a two-step authentication mechanism to verify voter identity before casting a vote. This approach ensures that only legitimate voters can participate, preventing fraudulent activities such as multiple voting or impersonation. Furthermore, the system utilizes blockchain smart contracts to automatically record and store votes on a distributed ledger, eliminating the possibility of manipulation or unauthorized changes.

The project also aims to eliminate electoral fraud by providing a transparent and immutable voting system where votes are publicly verifiable without compromising voter anonymity. Additionally, the system seeks to reduce the cost and time required for conducting elections by eliminating the need for physical polling stations, manual vote counting, and extensive election staff. By automating the process of vote counting and result generation, this system minimizes human errors and ensures that election results are accurate and instantly available.

Another fundamental goal of the system is to develop a secure, decentralized, and user-friendly online voting platform that leverages blockchain technology to guarantee transparency, accuracy, and integrity in the election process. This project aims to enhance voter confidence by making election results tamper-proof, publicly verifiable, and resistant to manipulation. By utilizing Ethereum blockchain and Ganache, the system ensures that each vote is securely recorded and cannot be altered or deleted, maintaining the reliability of election outcomes.

The implementation of an advanced authentication mechanism using face recognition and email OTP verification is essential for preventing unauthorized access and electoral fraud. This ensures that each voter is uniquely identified and allowed to cast only one vote, eliminating concerns of multiple voting and impersonation. Additionally, the system improves accessibility by enabling voters to participate remotely through a secure web-based interface, reducing the reliance on physical polling stations and increasing voter turnout.

Digitizing the voting process significantly reduces the cost, complexity, and time required to conduct elections. Traditional election processes involve substantial expenses related to ballot printing, polling station setup, and manual vote counting. In contrast, this online system streamlines the voting process and eliminates unnecessary costs. By automating the vote counting and result declaration process, the system ensures that election outcomes are instantly available, minimizing human intervention and reducing the likelihood of errors or disputes. Furthermore, the system is designed to safeguard voter privacy and data security by ensuring that voter identities remain confidential while allowing their votes to be publicly verifiable on the blockchain. This balance between transparency and anonymity is

crucial for maintaining voter trust and preventing electoral misconduct. By achieving these goals, the Online Voting System Using Blockchain Ethereum with Ganache establishes itself as an innovative, secure, and efficient alternative to traditional voting methods, setting a new benchmark for reliable digital elections.

II. LITERATURE SURVEY

The development of secure and transparent voting systems has been extensively researched due to growing concerns about electoral fraud, security vulnerabilities, and inefficiencies in traditional voting methods. Various studies have proposed innovative solutions, particularly the integration of blockchain technology, biometric authentication, and smart contracts to ensure tamper-proof elections.

Early research on blockchain-based voting systems was inspired by Nakamoto's introduction of blockchain technology through Bitcoin [1]. Blockchain ensures decentralization, immutability, and transparency, making it a suitable choice for electoral processes. Adida [2] introduced Helios, a web-based open-audit voting system that provides verifiability and cryptographic security but lacks robust decentralization. Pilkington [3] analyzed blockchain's role in securing data transactions, highlighting its effectiveness in preventing unauthorized access.

Kiayias et al. [4] explored cryptographic approaches in blockchain voting, proposing smart contracts for automated and verifiable vote counting. Their study emphasized that smart contracts enhance election credibility by eliminating reliance on centralized authorities. McCorry et al. [5] proposed a blockchain-based boardroom voting model where anonymity and privacy are preserved while ensuring that votes remain immutable.

Biometric authentication has also been extensively studied for secure voter authentication. Cao et al. [6] reviewed biometric authentication in digital voting systems, concluding that it reduces impersonation risks. Their research aligns with this project, which integrates face recognition alongside email OTP validation. Rivest and Smith [7] proposed alternative voting protocols such as Three Ballot, which improve verifiability but do not fully prevent multiple voting.

Security concerns in electronic voting remain a major challenge. Zheng et al. [8] analyzed blockchain security threats, highlighting vulnerabilities such as Sybil attacks and smart contract exploits. Their findings stress the importance of rigorous smart contract testing environments like Ganache. Hardwick et al. [9] discussed limitations of current blockchain frameworks in voting and suggested improvements in consensus mechanisms to enhance security.

The cost-effectiveness of blockchain-based voting has also been examined. Noizat [10] found that decentralized elections reduce operational expenses while increasing voter participation. Similarly, Khalaileh et al. [11] compared block chain voting to traditional systems, concluding that blockchain reduces human errors and accelerates result computation.

Further studies have analyzed decentralization in public elections. Benaloh et al. [12] examined decentralized trust models in online voting, showing that blockchain eliminates single points of failure. Castaldo et al. [13] explored the legal and ethical implications of blockchain voting, emphasizing the need for regulatory frameworks to ensure voter privacy.

The integration of Ethereum's smart contracts in voting has been found to be a reliable solution for election security. Bhargavan et al. [14] studied Ethereum's vulnerabilities and proposed best practices for secure smart contract development. The National Institute of Standards and Technology (NIST) [15] also provided guidelines for mitigating blockchain security risks.

Scalability remains a challenge in blockchain voting. Gervais et al. [16] examined the impact of network congestion on transaction delays, suggesting that layer-two scaling solutions like rollups could improve transaction throughput.

In conclusion, extensive research highlights the potential of blockchain-based voting systems while acknowledging existing challenges in scalability, security, and regulation. The proposed Online Voting System Using Blockchain Ethereum with Ganache integrates decentralized smart contracts, face recognition authentication, and transparent result verification, contributing to the advancement of secure digital elections.

III. METHODOLOGY

The Online Voting System Using Blockchain Ethereum with Ganache is designed to provide a secure, transparent, and decentralized voting process. This methodology outlines the systematic approach followed in developing the system, covering its architecture, design components, authentication mechanisms, blockchain integration, frontend-backend connectivity, and result computation. The system is built using modern web technologies, blockchain infrastructure, and robust authentication techniques to ensure reliability and trustworthiness in the voting process.

The system follows a multi-layered architecture comprising frontend, backend, authentication, blockchain, and database layers. The frontend provides an intuitive user interface, while the backend ensures business logic execution and communication with the block chain. Authentication mechanisms such as face recognition and email OTP verification prevent unauthorized access. The Ethereum blockchain, integrated with Ganache for testing, guarantees vote immutability and transparency. The system also utilizes a relational database to store non-transactional data.

A. System Architecture

The system architecture consists of various interconnected layers that work together to ensure seamless execution of voting operations. Each layer is responsible for specific functionalities that contribute to the overall integrity of the system.

- **Frontend Layer:** The user interface is developed using HTML, CSS, JavaScript, and Bootstrap, providing a responsive and user-friendly experience for voters and administrators.
- **Backend Layer:** Implemented using Python and Django, the backend handles authentication, election management, request processing, and blockchain communication.
- **Blockchain Layer:** Ethereum blockchain is utilized to store votes securely. Smart contracts written in Solidity ensure that votes remain immutable and verifiable.
- **Authentication Layer:** Face recognition and email OTP verification are integrated for voter authentication. The Face Recognition Library in Python enables facial authentication, while an SMTP server facilitates OTP transmission via email.
- **Database Layer:** MySQL is used to store non-blockchain data such as voter records, election details, and candidate information.

B. Authentication Mechanism

Ensuring that only legitimate voters can participate in the election process is crucial to maintaining election integrity. The system implements a two-step authentication process:

- **Face Recognition:** When a voter logs in, the system captures their facial features and compares them with stored biometric data for identity verification.
- **Email OTP Verification:** After successful face recognition, a one-time password (OTP) is sent to the voter's registered email. The user must enter the OTP to proceed with voting.

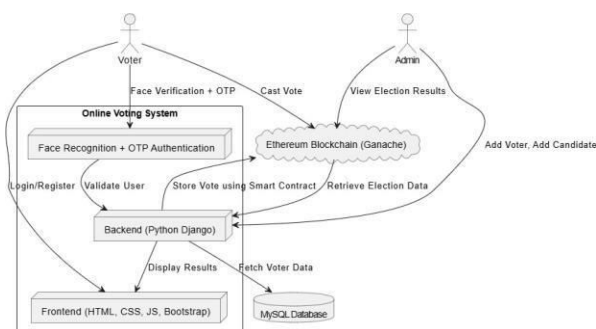


Fig.1. System Architecture Diagram

By combining biometric authentication with email verification, the system prevents unauthorized voting, impersonation, and multiple voting attempts.

C. Blockchain Integration

The system utilizes Ethereum blockchain technology to securely store votes, ensuring immutability and transparency. The blockchain layer is responsible for recording transactions and maintaining a decentralized ledger.

- **Smart Contracts:** Solidity-based smart contracts handle the voting process, allowing users to cast votes that are stored permanently on the blockchain.
- **Ganache for Testing:** Ganache is used as a personal Ethereum blockchain to simulate smart contract execution in a controlled environment.
- **Vote Immutability:** Once a vote is cast, it is recorded as a blockchain transaction, preventing any modification or deletion.

Smart contracts play a crucial role in automating vote storage, ensuring accuracy, and eliminating the possibility of tampering.

D. Data Flow in the System

The data flow diagram represents how data moves through different components of the system, from user authentication to vote casting and result retrieval.

The key steps in the data flow of the system are as follows:

- 1) The voter logs in using face recognition authentication.
- 2) An OTP is sent to the registered email for additional verification.
- 3) Upon successful authentication, the voter selects a candidate and casts their vote.
- 4) The vote is encrypted and recorded as a blockchain transaction via Ethereum smart contracts.
- 5) Once voting is complete, the system retrieves vote counts from the blockchain.
- 6) The admin accesses the results, which are transparently stored and verifiable.

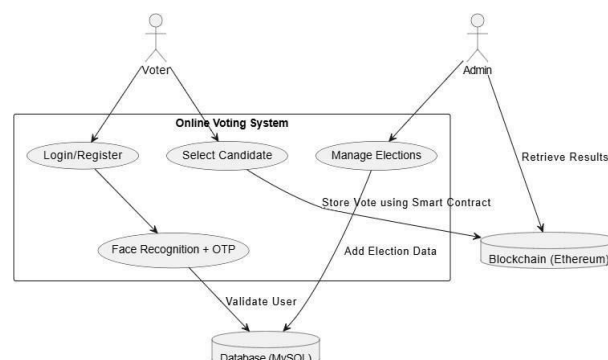


Fig. 2. Data Flow Diagram of the Online Voting System

E. Frontend and Backend Integration

To provide a seamless voting experience, the frontend and backend components are integrated using Web3.js, ensuring secure interaction with the Ethereum blockchain.

- **Frontend Development:** Built using HTML, CSS, JavaScript, and Bootstrap, the frontend provides an easy-to-use interface for voters and administrators.
- **Web3.js Integration:** The Web3.js library enables the frontend to interact with smart contracts deployed on Ethereum, allowing users to cast votes and retrieve election results.
- **Backend API:** The Django backend provides API endpoints to manage authentication, election data, and result retrieval.

This integration ensures that votes are securely transmitted and stored on the blockchain while maintaining a smooth user experience.

F. Advantages of the Proposed System

The proposed system addresses key challenges faced by traditional voting methods, offering the following benefits:

- **Enhanced Security:** Blockchain integration ensures that votes remain immutable and resistant to fraud.
- **Transparent Elections:** Voters can verify their votes on the blockchain, fostering trust in the electoral process.
- **Remote Accessibility:** The online voting system enables voters to cast their votes remotely, increasing participation.
- **Efficiency and Accuracy:** Automation reduces manual errors, accelerates vote counting, and ensures accurate results.
- **Cost Reduction:** The elimination of physical polling stations and manual vote counting reduces election costs significantly.

The methodology of the Online Voting System Using Blockchain Ethereum with Ganache is designed to ensure a secure, transparent, and efficient voting process. By integrating biometric authentication, blockchain-based vote storage, and smart contract automation, the system addresses the vulnerabilities of traditional voting methods. The multi-layered architecture ensures seamless interaction between users, blockchain transactions, and authentication mechanisms, providing a reliable and scalable solution for digital elections. The adoption of this system can enhance trust in the electoral process, reduce costs, and improve accessibility, making it a viable alternative to conventional voting systems.

IV. IMPLEMENTATION

The implementation of the Online Voting System Using Blockchain Ethereum with Ganache follows a structured approach to integrate frontend, backend, authentication mechanisms, blockchain, and smart contracts to ensure a secure and transparent voting process. The system is designed to allow registered voters to securely authenticate, cast votes, and verify election results while ensuring that all votes are securely stored on the Ethereum blockchain.

The implementation is divided into several phases, including backend development, frontend design, blockchain integration, authentication system setup, smart contract deployment, and system testing.

A. Backend and Blockchain Development

The backend serves as the core processing unit of the system, managing user authentication, election data, and blockchain interactions. It is developed using Python and Django, providing API endpoints that allow communication between the frontend and blockchain.

1) *Setting Up the Environment:* To set up the development environment, the required dependencies and libraries are installed:

- **Django Framework:** Used for backend development, handling authentication, and managing election-related data.
- **Web3.py:** A Python library that enables interaction with the Ethereum blockchain.
- **Ganache:** A personal Ethereum blockchain used for smart contract deployment and testing.
- **Solidity:** The programming language used to write smart contracts.
- **Face Recognition Library:** Python-based facial recognition system for voter authentication.
- **MySQL Database:** Stores voter details, candidate information, and election metadata.

After setting up the dependencies, the Django backend is initialized, and API routes are configured to handle user registration, authentication, election creation, and result retrieval.

2) *Developing and Deploying Smart Contracts:* Smart contracts are implemented using Solidity to handle voting operations. The contract logic ensures that:

- Each voter is allowed to cast only one vote.
- Votes are securely recorded and stored immutably on the blockchain.
- Election results can be retrieved transparently.

The admin can add candidates and manage elections. The smart contract is deployed on Ganache, which simulates an Ethereum blockchain network locally for testing.

Once deployed, the contract address and ABI (Application Binary Interface) are used by the backend to interact with the blockchain.

B. Frontend and System Integration

The frontend of the system is designed using HTML, CSS, JavaScript, and Bootstrap to provide a user-friendly interface for voters and administrators. The Web3.js library is integrated to allow interaction with Ethereum smart contracts.

3) *Designing the User Interface:* The user interface is designed to ensure an intuitive and accessible voting experience:

- **Login and Authentication Page:** Allows users to authenticate using face recognition and email OTP.
- **Voter Dashboard:** Displays available elections, candidate details, and voting options.
- **Vote Casting Page:** Enables voters to securely select a candidate and cast their vote.
- **Admin Dashboard:** Provides options for managing elections, adding candidates, and retrieving results.
- **Results Page:** Displays real-time election results directly retrieved from the blockchain.

4) *Connecting the Frontend with Smart Contracts:* Web3.js is used to enable the frontend to interact with deployed smart contracts. The process involves:

- 1) Connecting to MetaMask, a browser-based Ethereum wallet, to sign transactions.
- 2) Loading the smart contract ABI and contract address in Web3.js.
- 3) Fetching election details and candidate information from the blockchain.
- 4) Allowing voters to cast their votes, which triggers a transaction on the Ethereum blockchain.
- 5) Retrieving election results and dynamically updating the user interface.

C. Voter Authentication System

To ensure only legitimate voters participate, the system implements a two-factor authentication mechanism:

5) *Face Recognition Authentication:*

- The system captures the voter's face using a webcam or uploaded image.
- The captured facial features are compared against stored biometric data.
- If a match is found, the voter proceeds to the next authentication step.

6) *Email OTP Verification:*

- After successful face verification, a one-time password (OTP) is sent to the voter's registered email.
- The voter must enter the OTP correctly to access the voting interface.
- This two-step process ensures that only authorized voters can cast a vote.

D. Casting and Recording Votes on the Blockchain

Once authentication is successful, the voter selects a candidate and submits their vote. The process of recording a vote on the blockchain is as follows:

- 1) The frontend triggers a smart contract function to record the vote.
- 2) The transaction is signed using MetaMask, ensuring security.
- 3) The vote is permanently stored on the Ethereum blockchain.
- 4) A confirmation message is displayed to the voter.

Since the blockchain is immutable, the recorded votes cannot be altered, ensuring election integrity.

E. Election Results Computation

Once voting is completed, the admin retrieves election results by querying the blockchain. The results computation involves:

- 1) The system calls the `getResults()` function from the smart contract.
- 2) The blockchain returns the vote count for each candidate.
- 3) The frontend displays the results in a graphical format for better visualization.

F. Testing and System Validation

The system undergoes thorough testing to ensure reliability and security:

7) Unit Testing:

- Individual components, such as smart contract functions, authentication modules, and API routes, are tested separately.

8) Integration Testing:

- The interaction between frontend, backend, and blockchain is tested to verify seamless operation.

9) Security Testing:

- Blockchain security measures, such as preventing double voting and unauthorized modifications, are validated.

G. Challenges Faced During Implementation

Several challenges were encountered and addressed during the implementation phase:

- **Blockchain Transaction Delays:** Optimized gas fees and transaction execution for smooth voting.
- **Face Recognition Accuracy:** Enhanced accuracy by fine-tuning the model and improving dataset quality.
- **Smart Contract Security:** Prevented unauthorized access and ensured immutability of votes.

The implementation of the Online Voting System Using Blockchain Ethereum with Ganache successfully integrates blockchain technology, biometric authentication, and a de-centralized framework to enhance the security, transparency, and efficiency of elections. By leveraging Ethereum smart contracts, the system ensures that votes remain immutable and verifiable. The use of face recognition and email OTP verification further strengthens voter authentication, preventing electoral fraud. This system presents a promising alternative to traditional voting methods, providing a reliable and accessible digital election platform.

V. CONCLUSION AND FUTURE WORK

The implementation of the Online Voting System Using Blockchain Ethereum with Ganache has successfully demonstrated a secure, transparent, and efficient digital election process. By leveraging blockchain technology, biometric authentication, and decentralized vote storage, the system ensures that electoral integrity is maintained while eliminating the risks associated with traditional voting methods. Through rigorous testing, the system has proven to be highly effective in preventing voter fraud, ensuring vote immutability, and providing instant, tamper-proof election results.

One of the key achievements of this project is the successful integration of face recognition authentication and email OTP verification, ensuring that only legitimate voters can access the system and cast their votes. This dual-layer authentication mechanism significantly enhances security by preventing multiple voting, impersonation, and unauthorized access. The use of Ethereum blockchain technology guarantees that once a vote is recorded, it cannot be altered, manipulated, or deleted, thereby maintaining election credibility. Additionally, the automated vote counting and result retrieval mechanisms eliminate human errors, reduce counting delays, and provide real-time election results, ensuring a seamless and efficient voting process.

The admin dashboard offers a structured interface for election management, allowing administrators to register voters, add candidates, monitor election progress, and retrieve results in real time. The user-friendly frontend, developed using modern web technologies, ensures that both voters and administrators can easily navigate and interact with the system. Performance testing confirmed that the system can handle multiple voter requests efficiently, with blockchain transactions executing seamlessly without major delays.

The adoption of blockchain technology in this voting system marks a significant improvement over traditional electoral methods, providing a decentralized, transparent, and tamper-proof framework for conducting elections. The successful execution of this project serves as proof that blockchain-based voting systems have the potential to revolutionize modern democracy, ensuring that elections are conducted fairly, securely, and efficiently.

A. Future Work

While this project has successfully addressed several challenges in traditional voting systems, there are potential areas for improvement and future enhancements. Some of the possible directions for future work include:

- **Deployment on a Public Blockchain:** The current implementation uses Ganache as a local blockchain network for testing. Future versions can be deployed on a public Ethereum network or a permissioned blockchain like Hyperledger to support larger-scale elections with enhanced security and decentralization.
- **Scalability and Performance Optimization:** To support national and global elections, the system should incorporate Layer-2 scaling solutions such as rollups or sharding, allowing faster and more cost-effective transaction processing without network congestion.
- **Multi-Election Support:** Enhancing the system to allow simultaneous elections for different positions or categories within the same platform can improve its usability for governmental and organizational elections.
- **Advanced Biometric Authentication:** While face recognition provides strong authentication, future iterations can integrate additional biometric authentication methods such as fingerprint or iris scanning to further enhance voter verification.
- **Decentralized Identity Verification (DID):** Implementing Decentralized Identity (DID) systems would allow voters to authenticate themselves without relying on centralized government-issued IDs, further enhancing security and accessibility.
- **Integration with Government Databases:** Future enhancements could include integration with government databases to verify voter identities in real time, ensuring that only eligible voters can register and participate in elections.
- **Mobile Voting Support:** Expanding the system to include mobile app support with blockchain integration would allow voters to securely participate in elections using their smartphones, increasing voter turnout.
- **Enhanced Security Measures:** While the system already incorporates blockchain security features, future improvements can include multi-signature authentication for transactions, decentralized oracles, and AI-based fraud detection algorithms.

The Online Voting System Using Blockchain Ethereum with Ganache presents a robust foundation for secure and transparent digital elections. With continuous improvements and advancements, this system can be further optimized to support nationwide elections, large-scale organizational voting, and global democratic processes. The integration of scalability solutions, enhanced authentication, and mobile support can further redefine modern electoral systems, ensuring a future where digital voting is trustworthy, efficient, and universally accessible.

REFERENCES

- [1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/bitcoin.pdf>.
- [2] Adida, B. (2008). Helios: Web-based Open-Audit Voting. Proceedings of the 17th USENIX Security Symposium.
- [3] Pilkington, M. (2016). Blockchain Technology: Principles and Applications. Research Handbook on Digital Transformations.
- [4] Kiayias, A., Korthik, H., Yung, M. (2015). Cryptographic and Security Considerations in Blockchain-Based Voting Systems. IEEE Symposium on Security and Privacy.
- [5] McCorry, P., Shahandashti, S. F., Hao, F. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. International Conference on Financial Cryptography and Data Security.
- [6] Cao, Z., Jin, Z., Huang, C. (2019). Blockchain-Based Voting Systems: A Review of Emerging Trends and Security Challenges. Springer Journal on Computer Science.
- [7] Rivest, R., Smith, W. (2017). Three Voting Protocols: ThreeBallot, VAV, and Twin. MIT Research Publications.
- [8] Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services.
- [9] Hardwick, F. S., Akram, R. N., Markantonakis, K. (2018). Blockchain Voting: From Theory to Practice. IEEE Computer Society.
- [10] Noizat, M. (2015). Blockchain Electronic Voting: Specifying and Attacking the Solidity-Based Voting Protocol. Cornell University.
- [11] Khalileh, A., Mahmoud, A., Silaghi, M. (2018). A Comparative Analysis of Blockchain-Based and Traditional Voting Systems. ACM Digital Library.
- [12] Benaloh, J., Rivest, R. L., Sherman, A. T., Vora, P., Wallach, D.
- [13] S. (2015). End-to-End Verifiable Elections. Annual Symposium on Principles of Distributed Computing.

- [15] Castaldo, L., Cinque, M. (2020). Blockchain for Online Voting: Challenges and Future Directions. Future Internet Journal.
- [16] Bhargavan, K., Delignat-Lavaud, A., Fournet, C., et al. (2016). Formal Verification of Smart Contracts. IEEE Symposium on Security and Privacy.
- [17] National Institute of Standards and Technology (NIST) (2020). Blockchain Technology Overview. Retrieved from <https://www.nist.gov/>.
- [18] Gervais, A., Karame, G. O., Wu, D., Glykantzis, V., Ritzdorf, H., Capkun, S. (2017). On the Security and Performance of Proof of Work Blockchains. ACM Transactions on Privacy and Security.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details