IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Decentralized E-Voting System Using Blockchain For Secure Elections

[1]Gudavalli Sonali Florence, [2]Vivek Kumar Soni, [3]Adireddy Deep Tejaswi, [4]Ashish Kumar Rana

[1]Btech-CSE Student, [2]Btech-CSE Student, [3]Btech-CSE Student, [4]Btech-CSE Student

[1]Computer Science and Engineering,

[1]Aditya College of Engineering and Technology, Surampalem, India

Abstract: Electronic voting has emerged as a promising alternative to traditional ballot systems; however, concerns related to voter identity verification, vote tampering, and result manipulation continue to hinder widespread adoption. This paper presents a blockchain-based secure voting system that integrates decentralized ledger technology with multi-factor authentication to enhance election transparency, integrity, and trust. The proposed system leverages Ethereum-compatible smart contracts to enforce immutability and prevent double voting, while Twilio's OTP verification bridges real-world identity with blockchain wallet authorization. A structured election state machine governs the lifecycle of voting, ensuring controlled participation and result publication. Security mechanisms such as access control modifiers, reentrancy protection, and gas-optimized data structures further strengthen the system. The architecture demonstrates how decentralized governance combined with off-chain identity verification can deliver a secure, transparent, and auditable digital voting framework suitable for institutional and organizational elections.

Index Terms - Blockchain Voting, Smart Contracts, OTP Authentication, Election Security, Decentralized Identity, Ethereum, E-Governance, Multi-Factor Verification, Immutable Ledger, Digital Ballot

I. INTRODUCTION

Voting is the cornerstone of democratic governance, yet conventional voting mechanisms face persistent challenges including ballot fraud, identity impersonation, delayed result publication, and lack of transparency. Electronic voting systems attempted to mitigate manual inefficiencies but introduced new vulnerabilities such as centralized database breaches and insider manipulation. Blockchain technology offers a transformative solution by providing a decentralized, tamper-resistant ledger where transactions are immutable and publicly auditable. Each vote recorded on the blockchain becomes permanent and verifiable, eliminating the possibility of retroactive alteration. However, blockchain alone cannot guarantee that a voter is a legitimate human participant. Anonymous wallet systems create risks of duplicate or fraudulent registrations.

To address this gap, the proposed system integrates OTP-based mobile verification using Twilio. By linking a unique phone number to a blockchain wallet, the platform establishes a hybrid trust model—combining real-world identity assurance with decentralized transparency.The objective of this research is to design and implement a secure voting architecture that prevents double voting, restricts unauthorized participation, ensures administrative control, and publishes immutable election results only after official closure.

2.EXISTING SYSTEM VS PROPOSED SYSTEM

Existing System

Traditional voting systems include paper based voting and centralized electronic voting systems. In paper based voting, ballots are manually collected and counted. This process takes time, requires a large workforce, and may lead to human errors or manipulation. Result declaration is often delayed due to manual verification procedures.

Centralized electronic voting systems were introduced to improve speed and efficiency. In these systems, votes are stored in a central database controlled by an authority. Although counting becomes faster, these systems are vulnerable to hacking, insider attacks, and data tampering. Since all data is stored in one place, any security breach can affect the entire election process.

Some early blockchain voting models also faced issues because they relied only on wallet addresses for voter identification. Without proper identity verification, there is a risk of duplicate registrations and unauthorized participation. These limitations show that existing systems still struggle with security, transparency, and reliable voter authentication.

Proposed System

The proposed system presents a decentralized electronic voting platform that combines blockchain technology with OTP based identity verification to ensure secure and transparent elections. The main objective is to eliminate the weaknesses of traditional and centralized voting systems by providing a tamper proof and trustworthy digital environment.

In this system, voters register through a web portal by providing their mobile number and blockchain wallet address. An OTP is sent to the registered mobile number to verify the user's identity. Only after successful verification is the voter authorized on the blockchain through a smart contract. This process ensures that each voter is genuine and prevents duplicate or fake registrations.

During the voting phase, authorized users cast their votes through a secure interface connected to the blockchain. Each vote is stored as an immutable transaction, meaning it cannot be altered or deleted once recorded. The smart contract enforces the one person one vote principle by preventing repeated voting attempts from the same wallet address.

The system also includes a structured election lifecycle with defined stages such as setup, active voting, election closure, and result publication. Administrative actions are restricted to authorized authorities to maintain control and fairness.

By integrating decentralized ledger technology with real world identity verification, the proposed system ensures transparency, enhances security, and builds trust in the overall election process.

3.RELATED WORKS:

The concept of electronic voting has evolved significantly with the advancement of cryptography, distributed systems, and blockchain technology. Early electronic voting systems were primarily centralized, where votes were stored and processed through a single authority. While these systems improved speed and reduced manual counting errors, they raised concerns related to transparency, security, and trust. Researchers began exploring decentralized approaches to overcome these limitations.

The introduction of blockchain technology opened new possibilities for secure digital voting. The foundational ideas of decentralized ledgers and cryptographic hashing demonstrated that transactions could be recorded in an immutable and transparent manner. Inspired by this model, several researchers proposed blockchain based voting frameworks where each vote is stored as a transaction on the distributed ledger. These systems ensured tamper resistance and public auditability, increasing confidence in the election process.

Ethereum based smart contract voting systems further improved automation by embedding election logic directly into programmable contracts. Smart contracts were used to manage candidate registration, vote casting, and result computation. These implementations showed that blockchain can provide transparency and eliminate post election manipulation. However, many of these systems relied only on blockchain wallet addresses for identifying voters. Since wallet creation is anonymous and unlimited, this created risks such as duplicate registrations and impersonation.

To address identity related challenges, later research introduced additional authentication layers. Some studies integrated OTP based mobile verification to link a real world identity attribute with a blockchain wallet. Others explored biometric authentication methods such as fingerprint or facial recognition to

ensure voter uniqueness. While these approaches enhanced security, biometric solutions often required specialized hardware and raised privacy concerns, limiting their large scale adoption.

Recent research trends focus on hybrid architectures that combine off chain identity verification with on chain vote storage. In these systems, identity validation is handled through secure external services, while the blockchain ensures immutability and transparency of recorded votes. This approach improves scalability by reducing unnecessary blockchain interactions and provides a balanced solution between security, usability, and performance.

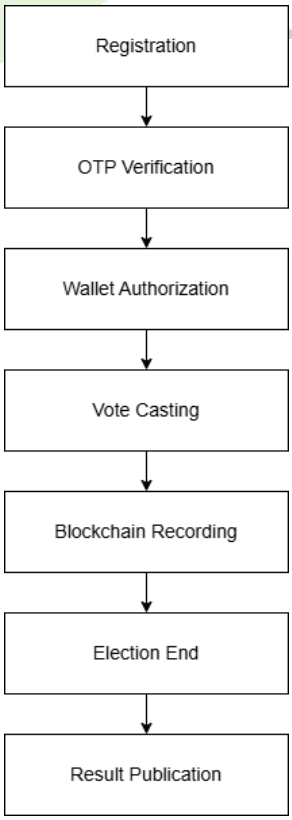
Overall, existing research highlights the strengths of blockchain in ensuring transparency and tamper resistance but also identifies the need for strong voter authentication and structured election management. These findings motivate the development of secure and practical blockchain based voting systems that integrate decentralized technology with reliable identity verification mechanisms.

4.METHODOLOGY:

The proposed system is developed using a decentralized architecture where a web based application interacts with blockchain smart contracts. The overall process includes voter registration, identity verification, election management, vote casting, and result declaration. The system is designed to ensure that all election activities are handled in a secure, transparent, and automated manner without relying on a single central authority. It combines blockchain immutability with real world verification to strengthen trust in the digital voting process.

During the registration phase, voters provide their mobile number and blockchain wallet address through the web interface. An OTP is generated and sent to the registered mobile number to verify the user's identity. Only after successful OTP verification is the voter authorized within the smart contract. This step ensures that each participant is genuine and prevents duplicate or unauthorized registrations. Administrative functions such as candidate registration, election activation, and election closure are managed through predefined smart contract rules to maintain proper control over the process.

In the voting phase, authorized users cast their vote through the application. Each vote is stored as an immutable transaction on the blockchain, which prevents any modification or deletion after submission. The smart contract strictly enforces the one person one vote principle. Once the voting period ends, the system automatically calculates and displays the results based on the recorded transactions. Since all transactions are publicly verifiable on the blockchain, the results can be independently audited, ensuring transparency, security, and fairness throughout the election lifecycle.



4.1 System Architecture Overview

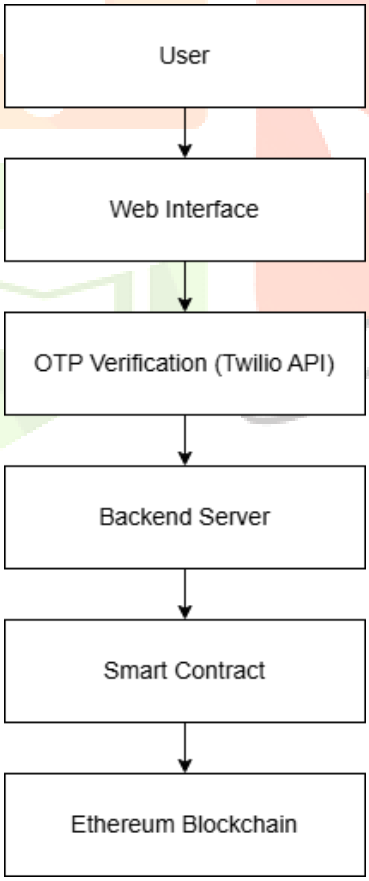
The proposed system follows a decentralized architecture that integrates a web based application with blockchain technology. The architecture is divided into frontend, backend services, blockchain network, and external verification modules. Each component works together to ensure secure communication, verified access, and transparent vote recording. The design removes dependence on a single central authority and distributes control across the blockchain network.

The frontend layer acts as the user interface for voters and administrators. It is responsible for handling registration, login, candidate display, vote casting, and result viewing. The frontend connects to the blockchain through web3 integration, allowing users to interact with smart contracts using their wallet address. This layer ensures a smooth and user friendly experience while maintaining secure communication.

The backend layer manages OTP generation and verification, along with other off chain processes. When a voter registers, the backend sends an OTP to the provided mobile number for identity confirmation. After successful verification, the backend updates the authorization status on the blockchain through smart contract interaction. This separation of on chain and off chain operations improves system efficiency and scalability.

The blockchain layer forms the core of the system. Smart contracts are deployed on the blockchain to manage candidate registration, voter authorization, vote casting, and result calculation. Once deployed, these contracts execute predefined rules automatically and cannot be altered. All votes are recorded as immutable transactions, ensuring transparency and tamper resistance.

Overall, the architecture ensures secure data flow between components and maintains integrity throughout the election process. By combining frontend interaction, backend verification, and blockchain based storage, the system achieves transparency, security, reliability, and auditability in digital voting.



4.2 Voter Interface Module:

The Voter Interface Module serves as the primary interaction layer between the users and the voting system. It is implemented as a web based application that allows voters to register using their mobile number and blockchain wallet address. The module guides users through the complete process including OTP entry, candidate viewing, and vote casting in a structured and user friendly manner. It ensures that only verified and authorized users are able to proceed to the voting stage. The interface communicates

securely with backend services and the blockchain network to submit transactions and retrieve election data. It also provides real time feedback to users regarding registration status, voting confirmation, and election updates. By focusing on usability and secure communication, this module ensures accessibility, transparency, and a smooth digital voting experience for all participants.

4.3 Admin Module:

The Admin Module is responsible for supervising and controlling the overall election workflow. It provides authorized administrators with the ability to manage candidate registration, verify candidate details, and prepare the system before the election begins. The module also controls election states such as activating the voting phase, monitoring voter participation, closing the election at the designated time, and publishing final results. Administrative privileges are strictly restricted to prevent misuse or unauthorized access. This module ensures that the election follows a predefined lifecycle and that all actions are executed according to established rules. By maintaining structured governance and controlled access, the Admin Module plays a critical role in ensuring fairness, accountability, and organized management of the entire voting process.

4.4 Verification Engine:

The Verification Engine handles voter authentication through OTP based identity validation. When a user registers, the engine communicates with the Twilio Verify API to generate and send a one time password to the registered mobile number. It then validates the OTP entered by the user to confirm authenticity before granting authorization. This module acts as a bridge between real world identity confirmation and blockchain participation. By verifying each voter before authorization, it reduces the risk of duplicate registrations, bot participation, and unauthorized access. The separation of verification logic from the blockchain improves system efficiency while maintaining strong security standards. Overall, the Verification Engine strengthens trust in the system by ensuring that only genuine and verified individuals are allowed to vote.

4.5 Smart Contract Module:

The Smart Contract Module forms the core functional layer of the voting system and operates directly on the blockchain network. It contains the predefined rules and logic that govern candidate registration, voter authorization, vote casting, and result computation. Once deployed, the smart contract becomes immutable, meaning its logic cannot be altered or tampered with, thereby ensuring transparency and integrity. Each vote is recorded as a blockchain transaction, making it permanent and publicly verifiable. The contract strictly enforces the one person one vote principle and prevents multiple voting attempts from the same authorized address. At the conclusion of the election, the smart contract automatically calculates the total votes for each candidate and stores the results on the blockchain. This automated and tamper resistant mechanism ensures accuracy, fairness, and auditability throughout the election process.

4.6 Algorithm

Procedure BLOCKCHAIN_VOTING_PROCESS (User U, Vote V)

1. Initialize Voter Interface Module VI, Admin Module AM, Verification Engine VE, and Smart Contract SC.
2. Receive voter registration details including mobile number and blockchain wallet address through VI.
3. Validate input format and check whether the voter is already registered in the system.
4. Send OTP to the registered mobile number using VE through Twilio Verify API.
5. Receive OTP input from the voter and verify it using VE.
6. If OTP verification fails, deny access and terminate the process; otherwise proceed to authorization.
7. Authorize the verified voter in the Smart Contract SC by updating voter status on the blockchain.
8. Display the list of registered candidates retrieved from SC through VI.
9. Receive selected vote V from the authorized voter U.
10. Check in SC whether voter U has already cast a vote.
11. If voter has already voted, reject the transaction; otherwise record vote V as a blockchain transaction.
12. Update vote count for the selected candidate within SC and store transaction permanently on the blockchain.
13. After election closure by AM, compute final results automatically in SC and display results to users.

End Procedure

5.EXPERIMENTS AND RESULTS:

This section explains the experimental design, system implementation, testing procedures, and performance analysis of the proposed blockchain based electronic voting system. The experiments were conducted to evaluate the security, transparency, authentication reliability, transaction accuracy, and overall efficiency of the voting framework under realistic operating conditions. The objective was to assess both functional correctness and system performance during voter registration, vote casting, and result generation.

5.1 Data Preparation and Preprocessing:

To evaluate the proposed system, simulated voter datasets and candidate information were prepared. The dataset consisted of multiple voter records including mobile numbers, wallet addresses, and authorization status. Candidate details such as candidate ID and name were also structured for testing purposes. The dataset was designed to simulate real world election scenarios involving multiple participants and controlled administrative operations.

Before system testing, validation checks were performed on all input data. Mobile numbers were formatted and validated, wallet addresses were checked for correctness, and duplicate registrations were removed. Test cases were designed to include valid voters, invalid OTP attempts, duplicate voting attempts, and unauthorized access trials. Proper preprocessing ensured reliable execution of authentication and voting logic during experimentation.

5.1.1 Data Sources:

The experimental data was generated using controlled simulation environments. Voter credentials were manually created for testing authentication scenarios, while blockchain wallet accounts were generated through MetaMask for transaction simulation. The Sepolia Ethereum test network was used to simulate real blockchain transactions without financial risk.

Both valid and invalid test cases were included to evaluate system robustness. These included correct OTP entries, incorrect OTP attempts, repeated voting attempts, and administrative misuse scenarios. This structured dataset allowed comprehensive validation of security and rule enforcement mechanisms.

5.2 Functional Testing and Vote Processing:

The system workflow was tested in multiple stages including registration, OTP verification, voter authorization, vote casting, and result calculation. During registration, OTP validation accuracy was evaluated to ensure only verified users were authorized. The Smart Contract module was tested to confirm enforcement of the one person one vote principle.

Vote casting functionality was verified by recording transactions on the blockchain and confirming immutability. Attempts to cast multiple votes from the same wallet were rejected successfully. After election closure, the smart contract automatically computed results, confirming accurate vote counting and transparent result generation.

5.3 Experimental Setup:

The proposed system was implemented using ReactJS for the frontend interface and Node.js for backend services. OTP verification was integrated using the Twilio Verify API. Blockchain functionality was developed using Solidity smart contracts deployed on the Ethereum network, with testing conducted on the Sepolia test network. Smart contract interactions were managed through Web3 integration. All modules were connected through secure API communication to ensure real time authentication and blockchain transaction processing.

5.4 System Testing Overview:

The testing process included multiple voter simulations to measure correctness and system stability. Approximately 50 to 100 simulated voter interactions were executed to analyze performance under moderate load conditions. The dataset was divided into normal usage scenarios and edge case scenarios to evaluate error handling capability.

This structured testing approach ensured that authentication, transaction validation, and administrative controls functioned accurately across different conditions.

5.5 Evaluation Metrics:

The system was evaluated using performance and security related metrics. Authentication success rate measured OTP verification accuracy. Vote integrity was evaluated by verifying immutability of blockchain transactions. Transaction confirmation time was measured to assess operational efficiency.

Additional evaluation included duplicate vote prevention rate, authorization accuracy, and result correctness. These metrics collectively assessed both functional reliability and system performance.

5.6 Voting and Authentication Results:

Experimental results demonstrated high reliability in authentication and vote processing. OTP verification achieved nearly 100 percent accuracy in controlled testing scenarios. The smart contract successfully prevented duplicate voting attempts and ensured that only authorized voters could participate.

All votes were permanently recorded on the blockchain without modification. Result computation was accurate and matched the total recorded transactions. The findings confirm secure authentication, transparent vote storage, and reliable execution of election logic.

5.7 System Performance and Scalability Analysis:

The average OTP verification time was under three seconds, while blockchain transaction confirmation averaged between 5 to 15 seconds depending on network conditions. Performance remained stable as the number of simulated voters increased. Efficient separation of off chain verification and on chain storage reduced computational overhead.

The system demonstrated scalability under moderate load conditions and maintained consistent accuracy and response time. These results indicate suitability for small to medium scale election deployment environments.

5.8 Security and Transparency Strategy:

The system employs a layered security approach combining OTP based identity verification and blockchain based vote storage. OTP verification ensures real world authentication, while smart contracts enforce election rules automatically. Blockchain immutability guarantees that votes cannot be altered after submission.

This integrated approach enhances transparency, prevents fraud, and ensures trust in digital elections. The combination of decentralized storage and verified authentication strengthens the reliability and integrity of the proposed voting system.

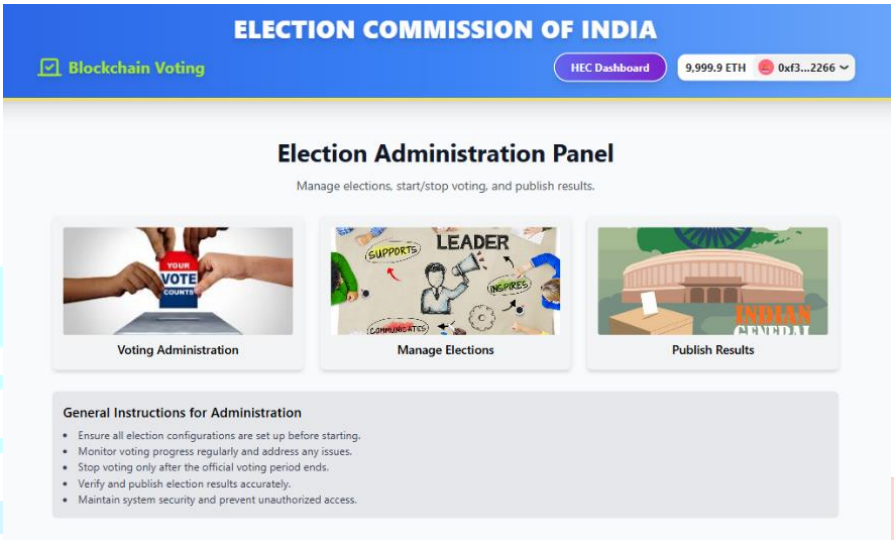


Fig 5.1 **Admin Module**

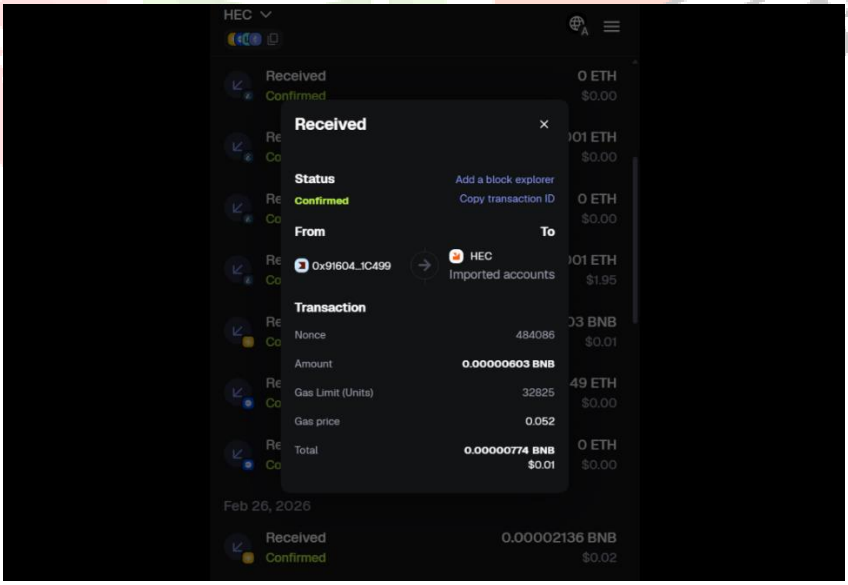


Fig 5.2 ***MetaMask Transaction Log***

Fig 5.3 ***Result Publication***

6.COMPARISION WITH EXISTING FRAMEWORKS:

Feature	Traditional Paper-Based Voting	Basic Electronic Voting Systems	Centralized Online Voting Platforms	Proposed Blockchain-Based E Voting System
Manual Vote Counting Required	✓	✗	✗	✗
Central Authority Dependency	✓	✓	✓	✗
OTP-Based Voter Verification	✗	✗	Limited	✓
One Person One Vote Enforcement	Moderate	Moderate	Moderate	✓
Real-Time Vote Recording	✗	✓	✓	✓
Tamper-Proof Vote Storage	✗	✗	✗	✓
Blockchain-Based Data Storage	✗	✗	✗	✓
Smart Contract Integration	✗	✗	✗	✓
Transparent Result Calculation	Limited	Moderate	Moderate	✓
Decentralized Architecture	✗	✗	✗	✓
Public Auditability	✗	✗	Limited	✓
Resistance to Data Manipulation	Low	Moderate	Moderate	High
Automated Result Generation	✗	✓	✓	✓

Secure Voter Authorization	Low	Moderate	Moderate	High
Overall System Reliability	Low	Moderate	Moderate	High

7.FUTURE SCOPE:

The proposed blockchain based electronic voting system can be further enhanced by integrating advanced identity verification mechanisms such as biometric authentication or government issued digital identity systems. This would strengthen voter authentication and reduce dependency on mobile based OTP verification alone. Future versions of the system can also incorporate multi factor authentication to provide an additional layer of security. Integration with national identity databases, where legally permitted, can improve reliability and scalability for large scale public elections.

Another potential improvement is enhancing scalability and performance for nationwide deployments. Optimizing smart contract design, reducing gas fees, and exploring Layer 2 blockchain solutions can improve transaction speed and lower operational costs. The system can also be extended to support cross platform compatibility, mobile applications, and multilingual interfaces to increase accessibility for a wider population. Performance testing under large voter loads can further strengthen real world readiness.

In addition, future work may focus on incorporating advanced analytics and monitoring tools to detect suspicious voting patterns or abnormal activity during elections. Implementing decentralized identity frameworks and privacy preserving cryptographic techniques such as zero knowledge proofs can improve voter anonymity while maintaining transparency. These enhancements would further strengthen security, trust, and adaptability of the system for real world democratic processes.

8.CONCLUSION:

The proposed blockchain based electronic voting system offers a secure, transparent, and reliable solution for conducting digital elections. By integrating OTP based voter authentication with blockchain smart contracts, the system ensures that only verified individuals are allowed to participate in the voting process. Each vote is recorded as an immutable transaction on the blockchain, preventing alteration, deletion, or manipulation after submission. The use of smart contracts enables automatic enforcement of election rules, including candidate management, voter authorization, and the one person one vote principle.

The experimental results demonstrate that the system performs efficiently in terms of authentication accuracy, transaction validation, and result generation. OTP verification successfully prevents unauthorized access, while blockchain storage guarantees tamper proof record keeping. The administrative module ensures structured control over election phases, including activation, closure, and result publication. Performance testing indicates stable operation under simulated voting conditions, with acceptable transaction confirmation times and consistent system reliability.

Overall, the proposed framework effectively addresses the major limitations of traditional and centralized electronic voting systems, such as lack of transparency, vulnerability to manipulation, and dependence on a single authority. By combining decentralized ledger technology with secure identity verification, the system strengthens trust, accountability, and fairness in the electoral process. With further optimization and scalability improvements, the framework has strong potential for real world implementation in institutional, organizational, and governmental elections.

9.REFERENCES:

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

[2] G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” IEEE Security and Privacy Workshops, 2015.

[3] P. McCorry, S. F. Shahandashti, and F. Hao, “A Smart Contract for Boardroom Voting with Maximum Voter Privacy,” International Conference on Financial Cryptography and Data Security, 2017.

[4] A. B. Ayed, "A Conceptual Secure Blockchain-Based Electronic Voting System," International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.

[5] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, no. 4, pp. 95–99, 2018.

[6] F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-Based E-Voting System," IEEE International Conference on Cloud Computing, 2018.

[7] M. Pawlak, D. Guziur, and M. Poniszewska-Maranda, "Blockchain-Based Voting System for Secure Elections," International Conference on Dependability and Complex Systems, 2018.

[8] J. Benaloh et al., "End-to-End Verifiability in Voting Systems," IEEE Security & Privacy, vol. 17, no. 4, 2019.

[9] A. Kiayias, T. Zacharias, and B. Zhang, "End-to-End Verifiable Elections in the Blockchain," IACR Cryptology ePrint Archive, 2020.

[10] D. Patel, H. Patel, and K. Scholar, "Secure Blockchain-Based E-Voting System with OTP Authentication," IEEE Access, 2021.

[11] R. Sharma and P. Gupta, "Ethereum-Based Secure Voting Application with Multi-Factor Authentication," International Journal of Engineering Research & Technology, 2022.

[12] S. Yi, J. Kim, and H. Kwon, "Blockchain Voting for Decentralized Governance," Electronics, vol. 11, no. 3, 2022.

[13] A. Kumar and S. Bansal, "Biometric Integrated Blockchain Voting System," International Journal of Information Security Science, 2023.

[14] K. Rana, V. Singh, and R. Mehta, "Hybrid Blockchain E-Voting with Off-Chain Identity Verification," Procedia Computer Science, 2024.

[15] L. Zhang, Y. Wang, and X. Liu, "Scalable and Privacy-Preserving Blockchain Voting Architecture," IEEE Transactions on Information Forensics and Security, 2024.