IJARSCT
ISSN: 2581-9429
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

Tamper-Proof Digital Voting Using Smart Contracts and Blockchain Technology

Prof. Minal Solanki[1], Aditya Shete[2], Pallavi Lanjewar[3]
Assistant Professor, Computer Application[1]
MCA, Computer Application[2,3]
, K. D. K College of Engineering, Nagpur, Maharashtra, India
minalsolanki@kdkce.edu.in[1], adityashete.mca23@kdkce.edu.in[2], pallavilanjewar.mca23@kdkce.edu.in[3]

Abstract: *Electronic voting (e-voting) systems are crucial for modern democracy, yet they often suffer from security vulnerabilities, lack of transparency, and centralized control, leading to potential election fraud. This paper proposes a blockchain-based e-voting system that enhances security, transparency, and voter privacy using advanced cryptographic techniques. The system leverages SHA-256 hashing for secure vote integrity, for decentralized and resilient storage of election data, and Zero-Knowledge Proofs (ZKP) to ensure voter eligibility without revealing personal identities, preserving the confidentiality of the electoral process. By utilizing blockchain's decentralized and tamper-resistant nature, the proposed system aims to eliminate single points of failure, prevent vote manipulation, and maintain voter anonymity.*

Furthermore, smart contracts automate critical processes such as vote validation, ballot recording, and result tallying, significantly reducing human intervention and minimizing the risk of manipulation or errors. The system ensures end-to-end verifiability, allowing voters to independently audit and verify that their votes were counted accurately without compromising the secrecy of their selections. Scalability and performance optimizations, including off-chain data handling and efficient consensus mechanisms, are incorporated to manage the demands of large-scale national or regional elections without degrading system performance. This research outlines the system's comprehensive architecture, detailed implementation strategies, and rigorous security analysis, addressing potential threats such as double voting, voter coercion, and denial-of-service attacks. Through simulation and case studies, the paper demonstrates the system's feasibility, efficiency, and resilience under various adversarial scenarios. By offering a transparent, secure, and user-friendly voting experience, the proposed blockchain-based e-voting solution has the potential to revolutionize digital elections and restore public trust in democratic processes worldwide.

Keywords: Blockchain, E-voting, Ganache, SHA-256, Zero-Knowledge Proofs, Smart Contracts, Immutable Ledger, Election Security

I. INTRODUCTION

The integrity and transparency of electoral processes are fundamental to the functioning of any democracy. However, traditional voting systems, whether paper-based or electronic, are often plagued by issues such as voter fraud, ballot tampering, logistical inefficiencies, and a lack of transparency in vote counting. These challenges have led to a growing distrust in electoral systems worldwide, necessitating the development of innovative solutions that can ensure secure, transparent, and accessible elections. Blockchain technology, characterized by its decentralized and unchangeable properties, has become a revolutionary asset for tackling these challenges, positioning it as a perfect base for a modern e-voting system.

A voting system based on blockchain technology utilizes distributed ledger capabilities to log every vote as a transaction on a secure and immutable platform. By using encryption and anonymization, the system protects voter privacy and inhibits duplicate votes or alterations. The inherent decentralization of blockchain removes the necessity for

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

a central authority, minimizing the risk of single points of failure and bolstering confidence in the election process. Furthermore, the immutability of blockchain ensures that once a vote is recorded, it cannot be altered or deleted, thereby safeguarding the integrity of the election results. One of the most significant advantages of this system is its ability to enhance voter accessibility and participation. By enabling remote voting through secure digital platforms, the system allows voters to cast their ballots from anywhere in the world, eliminating the need for physical polling stations. This is especially advantageous for individuals who encounter obstacles to voting, such as residents of isolated regions, individuals with disabilities, or those who cannot travel due to their jobs or health conditions. Transparency is another critical feature of blockchain-based e-voting. Unlike traditional systems where vote counting is often opaque and subject to human error or bias, blockchain allows for real-time verification of votes by all stakeholders. Each transaction (vote) is publicly recorded on the ledger, and anyone can audit the results without compromising voter privacy. This level of transparency fosters trust in the electoral process, as voters can be confident that their votes are accurately counted and that the final results reflect the true will of the electorate. The scalability of blockchain technology makes it suitable for elections of varying sizes, from local community polls to national elections. By leveraging permissioned or private blockchains, the system can be tailored to meet the specific needs of different electoral contexts while maintaining high levels of security and efficiency. Moreover, the use of blockchain can significantly reduce the costs associated with conducting elections, as it eliminates the need for physical infrastructure, paper ballots, and extensive manpower.

II. OBJECTIVE

The objectives of this project are

- **Ensure Transparency:** Use blockchain's decentralized and immutable ledger to prevent vote tampering and enhance trust.
- **Enhance Security:** Implement cryptographic techniques to prevent fraud, double voting, and unauthorized access.
- **Maintain Voter Privacy:** Use encryption methods to protect voter identities while ensuring votes are verifiable.
- **Enable Remote Voting:** Allow eligible voters to securely cast their votes from anywhere, increasing accessibility.
- **Automate Vote Counting:** Utilize smart contracts to validate, record, and tally votes instantly without human intervention.
- **Provide Real-Time Auditability**: Ensure that votes can be tracked and verified while preventing post-election modifications.
- **Reduce Operational Costs:** Minimize expenses related to ballot printing, polling stations, and manual vote counting.
- **Ensure Scalability:** Design a system capable of handling large-scale elections efficiently while maintaining security.

III. LITERATURE SURVEY

Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, Prathmesh Potdar (2020) Blockchain Technology-Based E-Voting System, ITM Web of Conferences, Vol. 32, ICACC 2020, Mumbai, Maharashtra.

This paper explores the feasibility of blockchain technology in electronic voting systems, focusing on security, transparency, and reducing electoral fraud.

Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan (2019) Secure Digital Voting System Based on Blockchain Technology, International Journal of Computer Science and Network Security (IJCSNS), Vol. 19, No. 12, 2019, NED University of Engineering and Technology, Pakistan.

The authors propose a secure digital voting system leveraging blockchain for enhanced authentication, vote integrity, and decentralized vote storage.

IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429 Volume 5, Issue 11, April 2025 Impact Factor: 7.67

Abhishek Subhash Yadav, Ashish Uttamrao Thombare, Yash Vandesh Urade, Abhijeet Anil Patil (2020) E-Voting Using Blockchain Technology, International Journal of Engineering Research & Technology (IJERT), Vol. 9, Issue 07, July 2020, MIT College of Engineering, Pune.

This study presents a blockchain-based voting framework aimed at eliminating traditional voting system drawbacks, such as tampering and lack of transparency.

Pooja Kumari, Bhagia Sheri, Isma Farah Siddiqui, Khubaib Khatri (2020) Conventional vs. Blockchain-Based E-Vote System, The 15th Asia Pacific International Conference on Information Science and Technology (APIC-IST), 2020, Mehran University of Engineering and Technology, Pakistan.

A comparative analysis of conventional electronic voting systems versus blockchain-based solutions, evaluating security, efficiency, and reliability.

Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, Hafiz Adnan Hussain (2022) A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems, Springer Nature - Journal of Supercomputing, 2022, analyzing authentication, data privacy, transparency, and verifiability challenges in blockchain-based voting.

This paper reviews scalability challenges in blockchain-based e-voting systems, focusing on authentication, data privacy, transparency, and verifiability.

IV. METHODOLOGY

This research adopts a practical, implementation-driven approach to design and develop a secure, transparent, and scalable blockchain-based e-voting system. The methodology is divided into several key phases: system design, technology stack selection, smart contract development, system integration, and testing. The Blockchain-Based Voting System developed using a systematic approach that integrates modern web technologies with decentralized blockchain architecture to ensure security, transparency, and efficiency in the electoral process. The methodology consists of the following key phases:

1. Requirement Analysis and System Planning: The project began with gathering requirements from potential users and stakeholders. Key requirements identified included:

- User authentication and role verification.
- Tamper-proof vote recording.
- Real-time result tracking.
- A transparent and auditable voting process.

A flowchart and system diagram were developed to visualize the user journey and system components.

2. Frontend Development: The user interface was developed using HTML, CSS, and JavaScript frameworks. Key features include:

- **Voter Portal**: Allows registration, login, and voting.
- **Admin Portal**: Enables user verification and election management.
- The interface was designed for ease of use and accessibility, especially for first-time users.

3. Backend Development and Smart Contract Integration: The backend was built using Node.js and Express, acting as a bridge between the frontend and blockchain.

- **Smart contracts** were developed using **Solidity** on the Ethereum blockchain.
- **Ganache** was used for local testing and simulation of the Ethereum network.
- Smart contracts were responsible for:
  - Voter registration
  - Vote casting
  - Counting and retrieving results

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

Ensuring one vote per verified user

4. Blockchain and Smart Contract Deployment: Ganache provided a personal Ethereum blockchain for testing. Key deployment steps included:

- Compiling and migrating contracts using **Truffle**.
- Connecting the frontend with Web3.js to interact with deployed smart contracts.
- Each voting action was stored as a transaction on the blockchain.
- Every transaction (vote) was mined and stored in a block, creating a permanent, tamper-proof ledger of all votes.

5. User Verification Mechanism: An admin verifies each registered user from the dashboard. Unverified users are restricted from voting. This introduces an essential level of oversight to deter fraud and unauthorized entry.

6. Voting Process Execution: Once verified, users can log in and cast their vote. The smart contract ensures:
A user can vote only once.

- Votes are counted instantly and transparently.
- Each transaction is traceable, adding auditability.

7. Result Visualization and Election Closure: Voting results are displayed in real-time using dynamic bar charts.
Votes are pulled from the blockchain using smart contract read functions.
Admin can officially end the election through the interface, locking further vote submissions

Cryptographic Security Techniques in Blockchain-Based E-Voting Systems

Cryptographic security forms the backbone of any blockchain-based e-voting system, ensuring that all aspects of the election process from voter authentication to vote casting and result verification are conducted with integrity, confidentiality, and authenticity. Through the incorporation of sophisticated cryptographic methods, the system protects against fraud, tampering, unauthorized access, and data breaches, while also guaranteeing the privacy and anonymity of voters. A key element in the system's cryptography is the SHA-256 (Secure Hash Algorithm 256-bit) hashing function. The SHA-256 converts input data, like voter identities and votes, into a fixed-length hash value that cannot be reversed. This ensures that no readable information is stored directly on the blockchain, maintaining voter privacy. The use of SHA-256 also makes the data tamper-evident—any slight modification in the original data results in a drastically different hash. This property makes it extremely difficult for attackers to alter previous voting records without detection. Moreover, each block in the blockchain includes the hash of the previous block, creating a secure, immutable chain that guarantees the chronological integrity of all recorded votes.

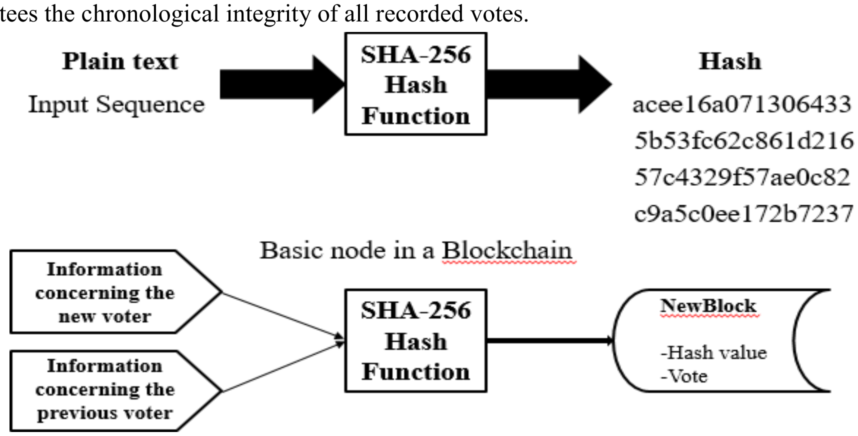

Fig. Role of SHA-256 in Blockchain-based E-Voting

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

Role of SHA-256 in Blockchain based E-Voting: SHA-256 plays a vital role in ensuring the integrity, security, and transparency of data within blockchain-based e-voting systems. This cryptographic hashing algorithm transforms voter information and voting data into fixed-length hash values, making even the smallest data alterations immediately noticeable. Because any change in the input results in a drastically different hash, SHA-256 serves as a powerful tool against unauthorized tampering. It also contributes to voter privacy by converting sensitive information into anonymized hashes before storing them on the blockchain. Furthermore, SHA-256 secures the blockchain structure by linking blocks through cryptographic hashes, maintaining the immutability of the voting record and protecting against fraudulent activities like double voting.

V. ARCHITECTURE

The system architecture follows a modular, decentralized model comprising three primary components: the frontend user interface, the backend server, and the blockchain network.

• Frontend (React.js): A web-based voting portal where users register, authenticate, and cast their votes through an intuitive interface. It communicates securely with the backend and blockchain.

• Backend (Node.js + Express): Handles business logic, user authentication, database interactions, and blockchain smart contract communication.

• Blockchain Layer (Ganache + Ethereum Smart Contracts): Stores immutable voting transactions and election smart contracts, ensuring transparency and tamper-resistance.

• Database (MySQL): Manages off-chain data such as user profiles, registration status, and session management, ensuring faster lookups without compromising blockchain integrity.

The system architecture of a blockchain-based e-voting system is composed of several integrated components designed to ensure a secure, transparent, and tamper-proof voting process. These components include the voter interface, authentication system, smart contract logic, blockchain ledger, consensus mechanism, and an administrative dashboard. Together, they work to eliminate vulnerabilities found in traditional voting systems while enhancing trust, accessibility, and integrity. At the core of the system lies the **smart contract**, which contains the essential logic that governs the entire voting process. It enforces predefined rules such as checking the validity of candidates, verifying voting eligibility, recording votes, and computing results. Functions like isValidCandidate(c), vote(v, c), voteIncrement(c), voteCount(c), and result() are executed by the smart contract in a transparent and deterministic manner. This automation removes the necessity for manual counting and minimizes the possibility of human error or tampering.

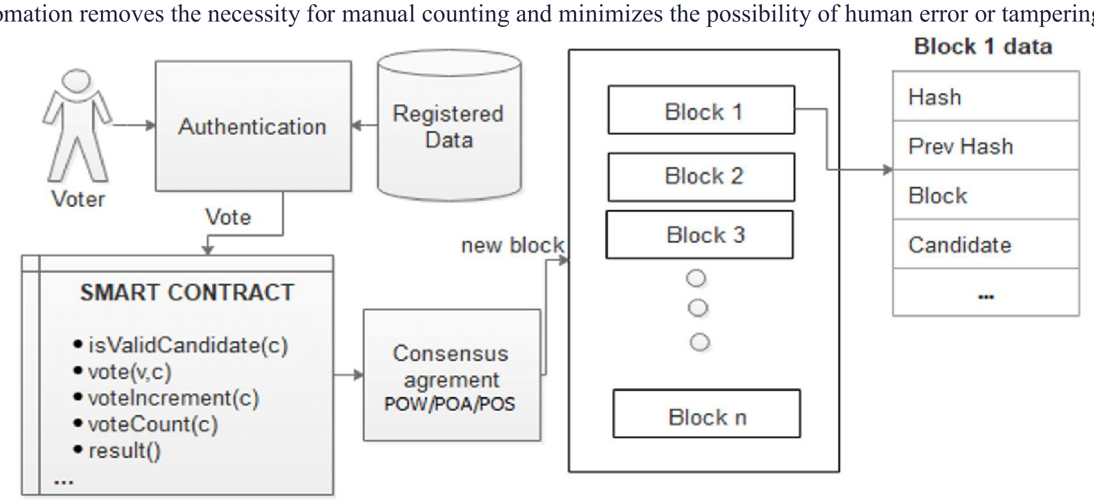

Fig. System Architecture

After a vote is cast, it gets packaged into a transaction and sent out to the blockchain network, where it is then validated. The system uses a **consensus mechanism** such as Proof of Work (PoW), Proof of Stake (PoS), or Proof of Authority (PoA) to confirm and secure the addition of the new vote block to the chain. Each block includes a

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

cryptographic hash, a reference to the previous block's hash, and the actual voting data. This linking of blocks forms an immutable and chronological ledger, ensuring that once a vote is recorded, it cannot be altered or deleted.

VI. EXPERIMENTAL RESULT AND FINDING

1. A user-friendly login interface was developed for the Blockchain-Based Voting System, enabling secure access through email and password authentication. The design incorporates essential features such as password recovery and new account creation, emphasizing accessibility and usability. This contributes to the overall security and efficiency of the voting system, aligning with the project's goal of providing a transparent and tamper-proof digital voting solution.

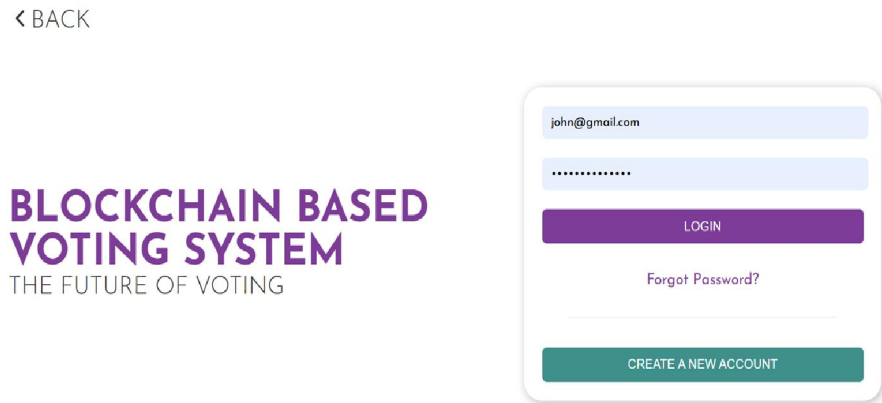

Fig. Login Page

2. An administrative interface was implemented to allow for the verification and management of user accounts within the Blockchain-Based Voting System. Admins can view registered users' details (name, email, phone number) and perform actions such as **VERIFY** or **DELETE** to maintain system integrity. This feature ensures that only authorized voters gain access, strengthening the security and reliability of the voting process

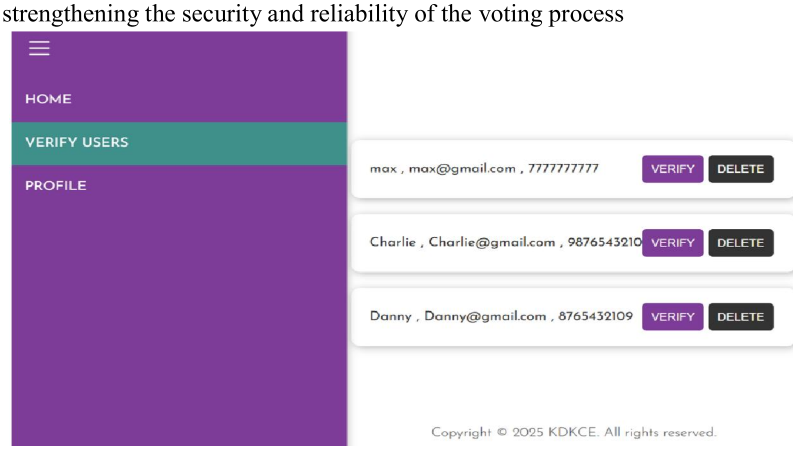

Fig. Admin authorized user verify

3. The voting interface successfully displays real-time results, showing the number of votes each candidate received. The admin can officially **end the election** using a dedicated control button, ensuring a transparent and verifiable conclusion to the voting process.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

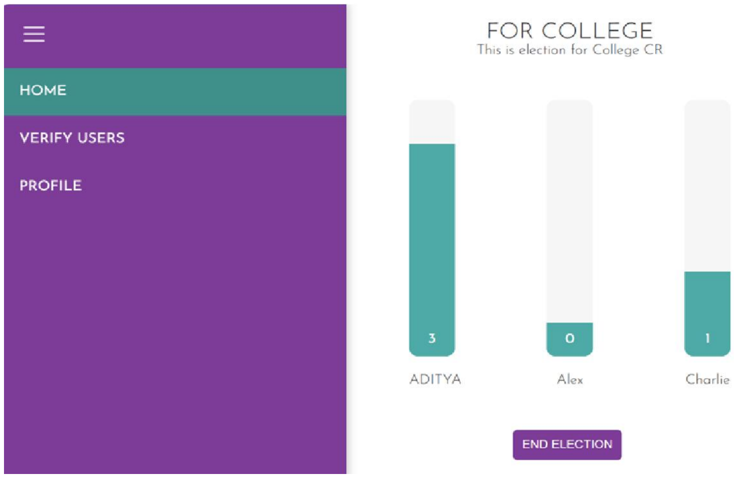

Fig. Count of Voting

4. The Ganache blockchain environment was utilized to simulate and validate transactions in the voting system. Each vote cast is recorded as a transaction within a block, ensuring transparency and immutability. As shown, blocks are mined sequentially with unique timestamps, gas usage, and transaction records, demonstrating the integration of blockchain technology in securely handling and storing voting data.

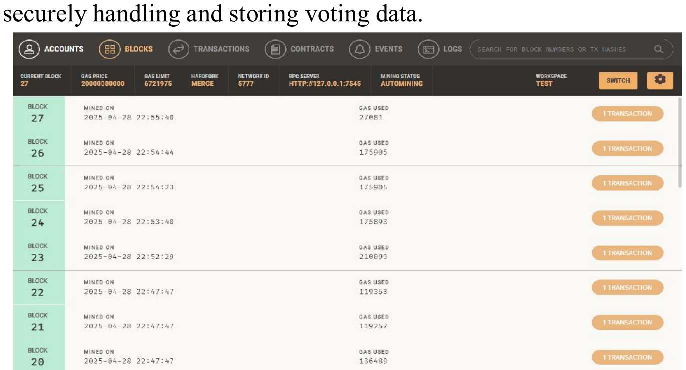

Fig. Ganache blockchain environment

VII. CONCLUSION

The suggested blockchain-based e-voting system tackles the key issues faced by traditional and electronic voting methods by utilizing decentralization, cryptographic security, and techniques that preserve voter privacy. By incorporating SHA-256 for maintaining data integrity, IPFS for decentralized data storage, and Zero-Knowledge Proofs (ZKP) for verifying voter identities, the system guarantees transparency, security, and anonymity. Furthermore, the implementation of smart contracts automates the counting of votes, minimizing human involvement and reducing the risk of manipulation. With its decentralized framework, the system decreases risks associated with vote tampering, centralized authority, and cyber threats, presenting a solid alternative to standard voting processes. The ability to verify votes in real-time boosts voter confidence, while the system's scalability ensures its applicability for elections of various magnitudes, ranging from local to national levels. Although there are benefits to using blockchain for e-voting, challenges remain, including issues with network scalability, adherence to regulations, and gaining user acceptance. In summary, this study shows that blockchain technology could transform the electoral process by providing a secure, transparent, and tamper-resistant voting system that maintains the integrity of democratic governance.

VIII. ACKNOWLEDGMENT

We express our sincere gratitude to our project guide, Prof. Minal Solanki, for her continuous guidance, valuable insights, and support throughout this research. Her expertise and encouragement have been instrumental in shaping this work. We would also like to thank the respected Dr. Anup Bhange, Head of the Master of Computer Applications (MCA) Department, as well as other faculty members for their helpful advice and guidance. Their support and encouragement have played a crucial role in the successful completion of this research. Furthermore, we extend our appreciation to our peers and mentors for their constructive feedback and discussions, which have helped refine our ideas. Lastly, we acknowledge the contributions of various researchers and authors whose work has served as a foundation for our study.

REFERENCES

[1] Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian, and Amol Kharat (2020). Blockchain-Based E-Voting System. Department of Computer Engineering, PCE, Navi Mumbai, India. SSRN. DOI: https://ssrn.com/abstract=3648870.

[2] Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, and Hafiz Adnan Hussain (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. Sensors, Vol. 22, 7585. DOI: https://doi.org/10.3390/s22197585.

[3] Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, and Prathmesh Potdar (2020). Blockchain Technology-Based E-Voting System. ITM Web of Conferences, Vol. 32, ICACC 2020, Mumbai, Maharashtra. DOI: https://doi.org/10.1051/itmconf/20203203001.

[4] Abhishek Subhash Yadav, Ashish Uttamrao Thombare, Yash Vandesh Urade, and Abhijeet Anil Patil (2020). E-Voting Using Blockchain Technology. International Journal of Engineering Research & Technology (IJERT), Vol. 9, Issue 07, July 2020. DOI: https://www.ijert.org.

[5] Pooja Kumari, Bhagia Sheri, Isma Farah Siddiqui, and Khubaib Khatri (2020). Conventional vs. Blockchain-Based E-Vote System. The 15th Asia Pacific International Conference on Information Science and Technology (APIC-IST), Mehran University of Engineering and Technology, Pakistan. DOI: https://www.researchgate.net/publication/343017419.

[6] Kashif Mehboob Khan, Junaid Arshad, and Muhammad Mubashir Khan (2019). Secure Digital Voting System Based on Blockchain Technology. International Journal of Computer Science and Network Security (IJCSNS), Vol. 19, No. 12, NED University of Engineering and Technology, Pakistan. DOI: https://core.ac.uk/display/155779036.

[7] Kavya Ramesh Naidu, Ankush Dinesh Ingale, Pratiksha Sukhadeo Gaikwad, Hitesh Rajendra Thakare, Sujal Sunil Chavan, and Prof. Yogeshk Sharma (2023). Online Voting System. International Research Journal of Modernization in Engineering, Technology and Science (IRJMETS), Vol. 5, Issue 5. DOI: https://www.doi.org/10.56726/IRJMETS38984.

[8] Krish Depani. (Year). Decentralized Voting System. GitHub Repository. Available at: https://github.com/Krish-Depani/Decentralized-Voting-System.