iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** III **Month of publication:** March 2025

DOI: https://doi.org/10.22214/ijraset.2025.67608

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

Block Chain Based Voting System

Mr. P. Hari Babu[1], Rajana Prasanna[2], Bejawada Deera Dhanunjay Veera[3], Bala Meghana[4], Cherukuri Hemanth[5]
Raghu Engineering College (REC), Department of Computer Science (Cybersecurity), Dakamarri, Bheemunipatnam, Visakhapatnam – 531162, India.

Abstract: ***This project aims to create a blockchain-based model that addresses key challenges in digital voting. The goal is to develop a secure and transparent system that eliminates common issues such as delays in result announcements, voter identity verification concerns, and security risks [1].***
Voting is the backbone of any democracy, and ensuring its integrity is crucial. Traditional digital voting systems often face problems like fraud, manipulation, and lack of transparency. Blockchain technology, with its decentralized and tamper-proof nature, offers a promising solution. It functions as a distributed ledger that records transactions securely in a peer-to-peer network, making it nearly impossible to alter past data [2]. This technology brings several benefits to voting, including decentralization, security, transparency, immutability, and voter anonymity [3]. A major highlight of this project is the integration of blockchain with smart contracts, which adds an extra layer of security and automation to the voting process [4]. The system is designed to work on the Ethereum blockchain, using smart contracts written in Solidity and accessed through blockchain wallets [5]. By eliminating the need for a central authority to oversee elections, this approach ensures a fair and transparent voting process where every vote is securely recorded and cannot be tampered with [6].
In essence, this project reimagines digital voting by leveraging blockchain's strengths, making elections more secure, efficient, and trustworthy.
Index Terms: blockchain technology, e-voting system, decentralization, smart contracts, Ethereum blockchain, transparency, security, immutability, distributed ledger.

I. INTRODUCTION

Democracy and the well-being of society go hand in hand, both relying on citizens' freedom and participation. Voting is a fundamental part of any democratic system, and for it to be effective, it must be transparent, fair, and secure [1]. A well-functioning election ensures that only eligible voters can cast their ballots, each person votes only once, and the results remain accurate and unaltered. However, bringing e-voting—whether blockchain-based or not—to a national level is challenging due to issues like scalability and the complexity of managing large-scale elections [2]. Given how crucial election results are, they also become attractive targets for manipulation and cyberattacks [3]. Interestingly, research shows that in university elections, the type of voting system plays a key role in voter participation. Students with a moderate level of trust in the system are more likely to vote compared to those with a high level of trust [4]. Countries like Estonia, Switzerland, and Norway were among the first to experiment with e-voting, but not without concerns. Estonia's system raised questions about transparency, while Switzerland's voting scripts were found to have security flaws that could allow ballots to be replaced with fraudulent ones [5]. Similarly, blockchain-based voting apps like Voatz have faced criticism for security vulnerabilities, making people question whether election results can truly be trusted [6]. Centralized blockchain voting systems also have their own risks, such as being vulnerable to cyberattacks like denial-of-service (DoS) attacks, which can disrupt the entire election process [2]. On the other hand, decentralized blockchain solutions require strong consensus mechanisms, which add complexity and could impact election outcomes [3]. One major concern with centralized e-voting systems is accessibility. Many people may not have the right devices, internet access, or digital skills to participate [4]. However, studies suggest that online voting can significantly increase turnout in university elections, potentially by more than 4% [5]. This is because students are generally more comfortable using digital platforms, and university elections are much smaller in scale than national ones. Universities often conduct elections for various positions, including student representatives, department heads, faculty members, and even the university rector. Traditional voting methods require a lot of effort—printing and managing ballots, setting up polling stations, and ensuring voters are present at the same time [6]. This can lead to long queues and disrupt academic activities. E-voting, on the other hand, makes the process smoother, reducing the chances of fraud while also making it easier for students to participate [1]. However, no voting system—whether paper-based or electronic—is completely secure. Even manual elections can be manipulated if organizers tamper with ballots to favor a particular candidate [2]. While national elections are at higher risk due to the significant political stakes, even university elections could be targeted, though the lower incentives may discourage large-scale fraud [3].

This paper proposes a blockchain-based e-voting system designed specifically for university elections. We explore the common challenges in existing research and present a structured solution to address them [4]. To ensure clarity, our system's design is formalized using UML diagrams [5].

The key contribution of this work is the development of a conceptual e-voting system that ensures voter privacy and security through a two-step process: voting and validation. Unlike blockchain-based financial transactions, which rely on complex consensus mechanisms like Ethereum or Hyperledger, our approach simplifies the process by using blockchain tables and a centralized database [6]. This removes the need for expensive and resource-intensive protocols, resulting in a more efficient, secure, and privacy-focused e-voting system tailored for universities.

II. RELATED WORK

1) Samuel A. Akinola – Blockchain Technology-Based E-Voting System

This study explores how blockchain can enhance the security and transparency of electronic voting. The author presents a decentralized ledger system that prevents vote tampering while ensuring voter anonymity and data integrity through cryptographic methods. Despite these benefits, challenges such as scalability and accessibility remain, particularly in large-scale elections. The paper suggests further research to refine blockchain-based voting for broader implementation.

2) Xiaojie Wang, Lei Zhang, Huiqin Zheng, and Jinghua Zhao – A Secure and Efficient Blockchain-Based E-Voting System

This research proposes a blockchain-based voting system designed to improve both security and efficiency. The authors introduce a hybrid consensus mechanism that blends Proof of Work (PoW) with Practical Byzantine Fault Tolerance (PBFT) to speed up transactions and enhance reliability. They also incorporate a verifiable secret-sharing technique to maintain voter privacy while securing the voting process. The system is tested for performance, showing its ability to handle large volumes of transactions efficiently, making it suitable for nationwide elections.

3) Amit Kumar, Pranjal Mishra, Ramesh Kumar, and Sanjay S. Patil – Blockchain-Based Secure Electronic Voting System

This paper focuses on building a secure electronic voting system using blockchain. The authors emphasize voter anonymity and preventing multiple votes from a single user by utilizing a permissioned blockchain. Smart contracts are employed to automate processes such as vote casting and counting, reducing human errors and increasing accuracy. Additionally, the system includes a real-time results feature, ensuring transparency in election outcomes.

4) Piyush Sharma and Kunal Gupta – Decentralized E-Voting System Using Blockchain

This study highlights the advantages of decentralizing e-voting systems through blockchain. The authors argue that a decentralized structure removes the risks of central authority manipulation and system failures. Their system relies on a public blockchain to ensure vote immutability, while cryptographic security measures like digital signatures protect voter identities. They also discuss key challenges, such as system scalability and ensuring that all voters, regardless of technical knowledge, can access the platform easily.

5) Rohit Patel – Survey on Voting System Using Blockchain Technology

This paper provides an in-depth analysis of blockchain-based voting models, examining their potential to solve issues like electoral fraud, vote tampering, and lack of transparency. The author reviews various approaches to implementing blockchain in elections and identifies major challenges, including technical barriers, regulatory concerns, and scalability limitations. The study concludes by emphasizing the need for further research to make blockchain-based voting more practical and accessible.

6) Dino Pavicevic – Blockchain-Based E-Voting System [6]

This research presents a private blockchain-based voting system focused on security, reliability, and ease of use. The system restricts access to verified participants and assigns role-based permissions to maintain election integrity. The author highlights how blockchain eliminates traditional election costs, such as paper ballots and manual vote counting, making the process more efficient and cost-effective. The study underscores the potential of blockchain in modernizing elections while acknowledging areas that require further development, such as voter authentication and system scalability.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

III. DESIGN AND METHODOLOGY

A. Objective

The goal of this project is to improve the security, transparency, and accessibility of digital voting using blockchain technology. Traditional voting systems face challenges such as voter fraud, tampering, and lack of transparency. By leveraging blockchain, we can create a more secure and reliable e-voting system that ensures every vote is recorded accurately and remains tamper-proof.

1) Objectives

To build a trustworthy voting system, it must meet the following key requirements:

- Transparency & Trust: The entire election process should be open and verifiable, allowing voters and officials to confirm its fairness.
- Vote Integrity: Once a voter casts their vote, it must be securely recorded and protected from any alterations.
- Voter Eligibility: Only registered and authorized voters should be allowed to participate, preventing fraud or duplicate voting.
- Security & Tamper Resistance: The system should be immune to hacking or manipulation, ensuring election results are legitimate.
- Decentralization: No single organization or entity should have control over the voting process, preventing bias or corruption.

2) How Blockchain Solves These Issues

Blockchain technology provides several advantages that make it ideal for secure e-voting:

- Secure Authentication: Only verified voters can cast their votes, ensuring fair participation.
- Privacy Protection: The system keeps voter identities anonymous, ensuring that votes cannot be traced back to individuals.
- Unchangeable Records: Once a vote is cast, it is permanently stored on the blockchain and cannot be modified or deleted.
- Easy Verification: The election results can be checked and verified by anyone, ensuring that the total number of votes counted is accurate and transparent.

By implementing blockchain in digital voting, we can restore trust in elections, eliminate fraud, and give voters confidence that their voices are truly heard.

Traditional electronic voting systems face challenges such as fraud, vote tampering, and lack of transparency. Blockchain technology offers a secure, verifiable, and tamper-resistant solution by ensuring that every vote is recorded permanently and transparently.

This methodology explains the step-by-step process of designing and implementing a decentralized e-voting **system** using Ethereum blockchain, Solidity smart contracts, MetaMask authentication, and SHA-3 hashing for security.

B. System Architecture

The voting system is structured into three main layers to ensure security, efficiency, and transparency.

1) Frontend Layer (User Interface)

- Built with React.js, HTML, CSS, and JavaScript to provide an intuitive voting experience.
- Features include voter registration, login, secure vote casting, and real-time result display.
- MetaMask integration ensures secure user authentication and vote transactions.

2) Backend Layer (Middleware)

- Developed using Node.js and Web3.js to act as a bridge between the frontend and blockchain.
- Handles voter authentication, vote submission, and election result retrieval.

3) Blockchain Layer (Core Security & Storage)

- Uses an Ethereum-based blockchain with Ganache for local development and testing.
- Smart contracts written in Solidity ensure election security, vote immutability, and transparency.
- SHA-3 hashing secures votes, making them tamper-proof and anonymous.
- The decentralized nature of blockchain eliminates single-point control or manipulation.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue III Mar 2025- Available at www.ijraset.com

C. Step-by-Step Implementation

Step 1: Define System Requirements

- Identify and address key concerns: fraud prevention, vote integrity, and transparency.
- Ensure that the system supports secure authentication, anonymity, and verifiability.

Step 2: Design System Components

User Roles

- Admin: Manages elections, registers candidates, and controls voting sessions.
- Voter: Registers, logs in via MetaMask, casts a secure vote, and views results.

Voting Flow

- The admin starts the election.
- Voters register and log in securely.
- Voters cast their votes, which are hashed using SHA-3.
- The hashed votes are stored on the blockchain.
- Election results are calculated and displayed transparently.

Step 3: Develop Smart Contracts

Smart contracts written in Solidity handle:

Voter registration and authentication to ensure only eligible voters participate.

Secure vote casting and storage to prevent fraud and duplication.

Automated result calculation for fast and accurate outcomes.

Step 4: Build the User Interface

- A React.js-based frontend allows voters to interact with the system easily.
- MetaMask authentication ensures that only verified users can vote.

Step 5: Secure the Voting System with SHA-3

- SHA-3 (Secure Hash Algorithm 3) is used to secure and encrypt votes.
- Once a vote is cast, SHA-3 generates a unique, irreversible hash.
- Collision resistance ensures that no two different votes produce the same hash, preventing duplication or manipulation.
- The hashed vote is then stored on the blockchain, making it immutable.

Step 6: Connect the Frontend with Blockchain

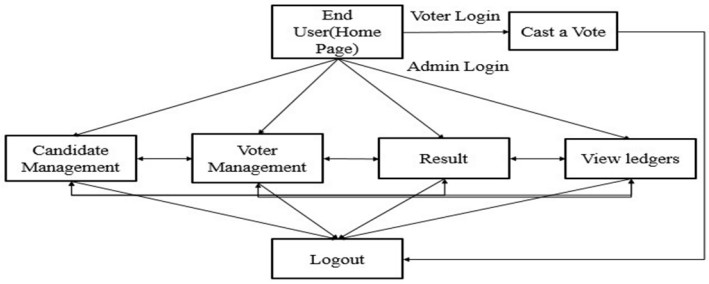
- Web3.js is used to establish communication between the frontend and the blockchain.
- This enables real-time vote submission, verification, and result display.

Step 7: Testing and Debugging

- Smart contracts are tested using Truffle and Ganache to ensure security and functionality.
- The system is checked for voting errors, security vulnerabilities, and transaction issues.

Step 8: Deployment and Execution

- The smart contract is deployed on an Ethereum test network (e.g., Rinkeby).
- The frontend is hosted on a web server, making it accessible to voters.



System Architecture

D. SHA-3 Hashing: Enhancing Security

SHA-3 is a cryptographic hashing algorithm that strengthens vote security by ensuring immutability, anonymity, and fraud resistance.

1) How SHA-3 Works in Voting?

a) Vote Submission & Hashing

When a voter selects a candidate, their vote is combined with a unique voter ID before being passed through the SHA-3 algorithm:

SHA3("Candidate A + VoterID") → Unique Hash

b) Storing the Vote Securely

- The hashed vote is stored on the blockchain, ensuring it cannot be modified or deleted.
- If anyone tries to tamper with a vote, the hash will change completely, making fraud easy to detect.

.

Feature	Why It Matters?
Immutability	Votes remain unchangeable once hashed.
Tamper-Proofing	Any modification to a vote results in a different hash, exposing fraud.
Privacy	Votes are stored anonymously without revealing voter identities.
Accuracy	No two different votes will ever generate the same hash.
Decentralization	Ensures that no single authority can manipulate votes.

By using SHA-3 hashing, the voting system achieves unmatched security and reliability, ensuring that elections are fair, transparent, and resistant to tampering.

```
FUNCTION SHA3(message, output_bits):
  // Convert message to binary representation
  message_bits = ConvertToBinary(message)

  // Padding: Append '1', followed by '0's, then '1' at the end
  message_bits = PadMessage(message_bits)

  // Initialize a 5x5 state matrix filled with zeros
  state = Matrix(5x5, 0)

  // Absorption phase: XOR message blocks into the state
  FOR each block in message_bits:
    state = XOR(state, block)

  // Apply Keccak-f permutation
  state = KeccakF(state)

  // Extract hash output
  hash_output = ExtractBits(state, output_bits)
  RETURN ConvertToHex(hash_output)
END FUNCTION
```

PSEUDOCODE FOR SHA3

2) How SHA-3 Works

SHA-3 (Secure Hash Algorithm 3) is a cryptographic hash function that processes input data of any length and generates a fixed-length hash output. Unlike SHA-256, which follows the Merkle-Damgård construction, SHA-3 is built on the Keccak sponge construction, making it more secure against certain attacks.

No matter how large or small the input is, the output remains consistent in length—typically 224, 256, 384, or 512 bits.

Key Properties of SHA-3

Consistency (Deterministic Behavior):

Every time you input the same data, you get the exact same hash output. This ensures reliability and integrity in cryptographic operations.

Fast Processing: SHA-3 is designed for quick computations, making it efficient for large datasets and blockchain applications.

Pre-Image Resistance: It is practically impossible to reverse-engineer the original data from a given hash. This ensures that even if someone intercepts the hash, they cannot determine the input.

Avalanche Effect (Sensitivity to Small Changes): Even a minor change in the input (like altering a single character) drastically changes the entire hash output, making it highly secure.

Collision Resistance:

SHA-3 ensures that no two different inputs produce the same hash. This prevents security breaches where multiple inputs could generate identical hash values.

Sponge Construction – A More Secure Approach:

Instead of using traditional block processing like SHA-256, SHA-3 follows the sponge construction model:

Absorbing Phase: The input is processed into an internal state.

Permutation Function: The internal state undergoes multiple transformations for added security.

Squeezing Phase: The final hash is extracted from the processed state.

This approach makes SHA-3 more resistant to attacks like length extension, which can be an issue with earlier SHA algorithms.

Why SHA-3 is Important in Blockchain

Enhanced Security: Blockchain relies on hashing to maintain data integrity. SHA-3's advanced cryptographic structure makes it more secure than older SHA versions.

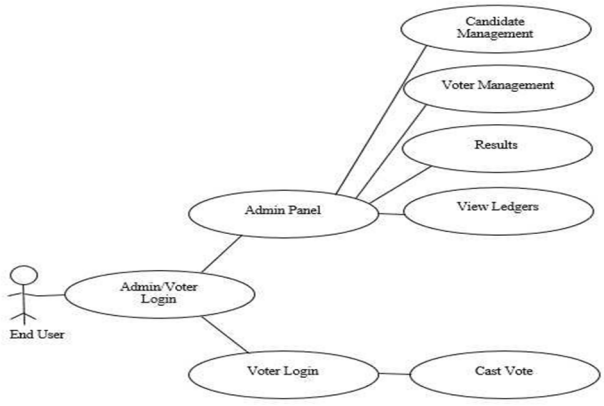
Tamper-Proof Mechanism: Every block in a blockchain contains a hash linking it to the previous block. If someone tries to alter data in one block, the hash changes, breaking the chain's integrity.

Future-Proofing: SHA-3 is designed to be more resistant to potential quantum computing threats, ensuring long-term security for blockchain networks.

Uses SHA-3 hashing to secure votes and ensure privacy.

As cybersecurity threats continue to evolve, the adoption of SHA-3 ensures robust protection for sensitive data, reinforcing trust in cryptographic systems.

Its ability to handle diverse security needs while maintaining high efficiency and reliability makes it a crucial tool in modern encryption techniques.



Use Case Diagram

This diagram represents a voting system and shows how different users interact with it. It includes an end user, who can be either an admin or a voter.

The process starts with the admin or voter logging into the system. If the user is an admin, they gain access to the admin panel, where they can manage candidates, handle voter registrations, view election results, and check voting records. These functions help ensure that the election runs smoothly and transparently.

If the user is a voter, they proceed to the voter login section, where they can access the option to cast their vote. This step ensures that only registered users can participate in the election process.

Lines connecting these actions indicate which users can perform specific tasks. Both admins and voters must log in, but their available options differ based on their roles. Admins oversee the election process, while voters focus on submitting their votes.

This UML diagram helps visualize the overall structure of the voting system in a clear and organized way, making it easier to understand how the system operates. Let me know if you need any modifications or additional details.

IV. RESULT

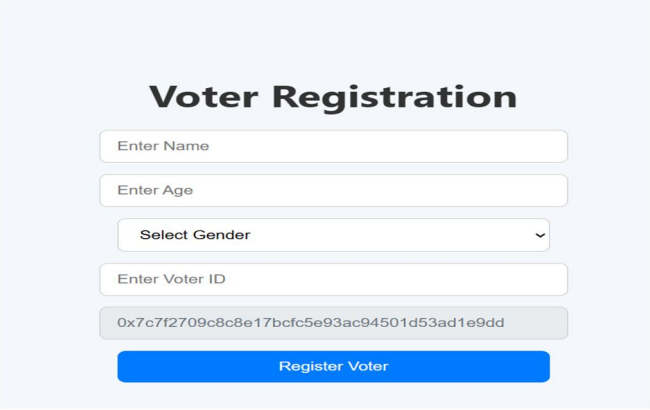
The following outcomes were observed after successfully implementing the Blockchain-Based Voting System:

A. Candidate Registration

Candidate registration is a critical step in ensuring only legitimate candidates participate in the election. The system successfully allowed authorized personnel to register candidates on the blockchain. The use of smart contracts ensured that only designated administrators could add candidates, preventing unauthorized modifications. Once registered, the candidate information was permanently recorded on the blockchain, eliminating the risk of tampering or manipulation. The decentralized nature of the system allowed voters and election officials to verify the candidate list at any time, increasing transparency.

B. Voter Registration and Authentication

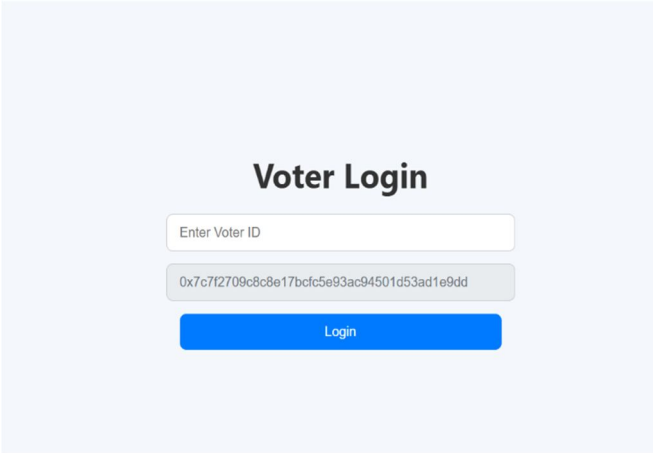
To ensure fair elections, the system implemented strict voter registration and authentication mechanisms. Each voter was assigned a unique wallet address using MetaMask, preventing multiple registrations under the same identity. The integration of MetaMask also ensured secure login and transaction signing, preventing unauthorized access. Voter lists were stored on the blockchain, making them verifiable and immutable, reducing the risk of fraud. Since the system operates in a decentralized manner, voter authentication was conducted without reliance on a central authority, reducing the risk of data breaches and identity theft.



C. Casting Votes

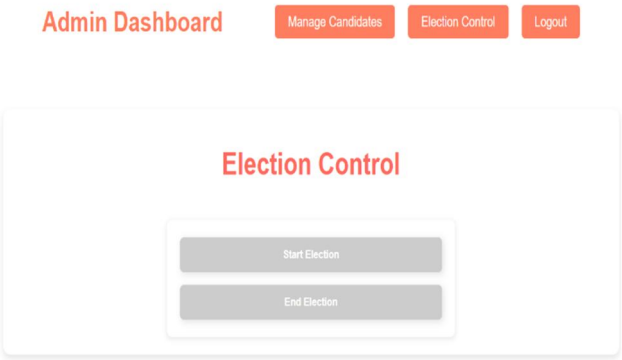
The system successfully enabled voters to cast their votes securely and transparently through a decentralized application. Smart contracts ensured that each voter could only vote once, preventing duplicate votes. The Ethereum blockchain recorded votes instantly, allowing real-time verification and eliminating delays in counting. Since each vote was hashed using SHA-3 before storage, voter anonymity was preserved while ensuring vote integrity. The system provided a transparent mechanism for verifying transactions without exposing voter identities, ensuring trust in the election process.

In a blockchain-based voting system, security and transparency are crucial. One of the most efficient ways to ensure voter authentication is by linking a voter's ID to MetaMask, a popular cryptocurrency wallet that interacts with blockchain networks.



D. Election Lifecycle Management

The system successfully allowed the administrator to start, pause, and end elections using smart contracts. This ensured that the voting process was well-regulated and transparent, preventing unauthorized changes. Once the election started, only registered voters could participate, ensuring that every vote was legitimate. At the end of the voting period, the admin finalized the election, preventing any additional votes from being cast. Since all votes were recorded on the blockchain, they became permanent and unalterable, making the entire process secure and tamper-proof. This approach eliminated concerns about manipulation, ensuring a fair and trustworthy election process.



E. Result Declaration

Once the election ended, votes were automatically counted using smart contracts. Since blockchain transactions are transparent and immutable, the system ensured that results were calculated instantly and without errors. Unlike traditional elections, where results might be delayed or subject to human error, this system provided immediate and accurate outcomes. The results were stored securely on the blockchain, preventing any form of alteration or tampering. Anyone—including voters, administrators, and auditors—could independently verify the election results, increasing confidence in the fairness of the process.

F. Security and Transparency

By using blockchain technology, the system eliminated the need for a central authority, reducing the risk of fraud or manipulation. In traditional voting systems, results are often controlled by a single organization, which can lead to bias or interference. This system distributed control across multiple nodes, ensuring that no single party could modify or manipulate votes.

To protect voter privacy, the system used SHA-3 hashing, which ensured that votes were recorded securely without revealing the identity of the voter. Each voter could verify that their vote was counted correctly without compromising their anonymity. Additionally, since the blockchain is publicly accessible, election transparency was significantly improved. Any attempt to alter the votes would be immediately visible, making it impossible to manipulate results without detection.

V. CONCLUSION

This blockchain-based voting system successfully addressed key vulnerabilities in traditional voting, ensuring that elections were secure, transparent, and resistant to fraud. By leveraging blockchain, it provided a trustworthy and efficient solution for modern digital voting. The combination of smart contracts, decentralized data storage, and cryptographic security ensured that every aspect of the election process—from voter authentication to result declaration—was fair and tamper-proof. With further enhancements, such as mobile integration and public blockchain deployment, this system could be scaled for large-scale elections, ensuring a future of secure digital democracy.

A. Challenges and Future Scope

Blockchain-based voting ensures security and transparency but faces challenges in adoption.

B. Scalability

Large-scale elections may lead to delays and high processing costs. Optimizing blockchain networks can help improve efficiency.

C. User Adoption

Many voters are unfamiliar with blockchain technology. A user-friendly interface and awareness campaigns can simplify participation.

D. Regulatory Issues

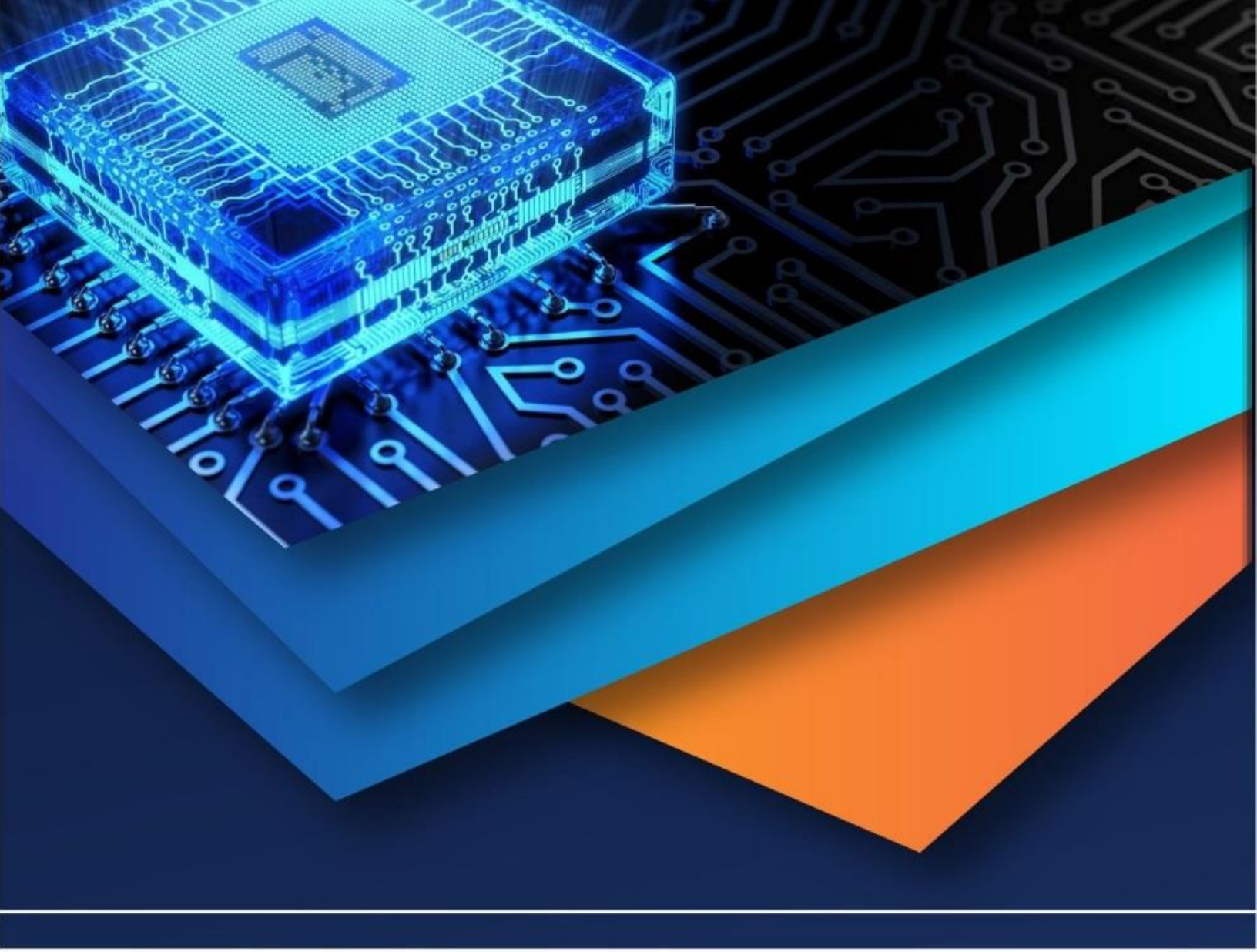
Governments need to update election laws for digital voting. Ensuring voter privacy and data security is essential for legal acceptance.

E. Future Scope

Enhancing mobile accessibility and security features can make blockchain voting more practical, leading to a secure and transparent election process.

REFERENCES

[1] S. A. Akinola, "Blockchain technology-based e-voting system," ResearchGate, 2020. [Online]. https://www.researchgate.net/publication/343285210_Blockchain_technology_based_e-voting_system
[2] X. Wang et al., "A Secure and Efficient Blockchain-Based E-Voting System," IEEE Xplore, 2023. [Online]. https://ieeexplore.ieee.org/document/10049991
[3] A. Kumar et al., "Blockchain-Based Secure Electronic Voting System," IRJET, vol. 10, no. 5, 2023. https://www.irjet.net/archives/V10/i5/IRJET-V10I519.pdf
[4] P. Sharma and K. Gupta, "Decentralized E-Voting System Using Blockchain," IRJET, vol. 10, no. 1, 2023. https://www.irjet.net/archives/V10/i1/IRJET-V10I147.pdf
[5] R. Patel, "Survey on Voting System Using Blockchain Technology," IJERT, vol. 11, no. 4, 2022. https://www.ijert.org/research/survey-on-voting-system-using-blockchain-technology-IJERTV11IS040130.pdf
[6] D. Pavicevic, "Blockchain-Based E-Voting System," RIT Croatia, 2022. https://www.rit.edu/croatia/sites/rit.edu.croatia/files/docs/3%20Pavicevic%20-%20Blockchain-based%20e-voting%20system.pdf
[7] S. Shah, Q. Kanchwala, and H. Mi. (2016). Block Chain Voting System. Economist. [Online]. Available: https://www.economist.com/sites/default/files/northeastern.pdf
[8] S.Park,M.Specter,N.Narula,andR.L.Rivest,‘‘Goingfrombadtoworse: From internet voting to blockchain voting,’’ J. Cybersecurity, vol. 7, no. 1, pp. 1–15, Feb. 2021, doi: 10.1093/cybsec/tyaa025.
[9] K. M. Khan, J. Arshad, and M. M. Khan, ‘‘Secure digital voting system based on blockchain technology,’’ Int. J. Electron. Government Res., vol. 14, no. 1, pp. 53–62, Jan. 2018, doi: 10.4018/IJEGR.2018010103.
[10] C. K. Adiputra, R. Hjort, and H. Sato, ‘‘A proposal of blockchainbased electronic voting system,’’ in Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS), Oct. 2018, pp. 22–27, doi: 10.1109/WorldS4.2018.8611593.
[11] A. Barnes, C. Brake, and T. Perry. Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers-Plymouth University. Accessed: Feb. 14, 2022. [Online]. Available: https://www.economist.com/sites/default/files/plymouth.pdf
[12] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K.-R. Choo, ‘‘The application of the blockchain technology in voting systems: A review,’’ ACM Comput. Surv., vol. 54, no. 3, pp. 1–28, Apr. 2022, doi: 10.1145/3439725.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY