iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** II **Month of publication:** February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77494

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 14 Issue II Feb 2026- Available at www.ijraset.com

A Smart Contract-Driven Blockchain Architecture for Secure Digital Voting

Smit Pingale[1], Vedanshi Gosalia[2], Divya Karotra[3], Riya Gajra[4], Sangita Bhoyar[5]
[1, 2, 3, 4]*Student, Department of Computer Engineering, V.E.S. Polytechnic, Mumbai, India*
[5]*Lecturer, Department of Computer Engineering, V.E.S. Polytechnic, Mumbai, India*

Abstract: ***In democratic systems, secure and transparent voting mechanisms are essential to maintain public trust and electoral integrity. Traditional paper-based and centralized electronic voting systems often face challenges such as limited transparency, risk of data manipulation, and dependence on centralized authorities. To address these issues, this project proposes a decentralized blockchain-based voting system designed to enhance security, transparency, and reliability. The system is developed on the Ethereum blockchain, where each vote is recorded as an immutable transaction to prevent tampering or duplication. Smart contracts written in Solidity automate essential election functions including voter registration, vote validation, and result computation. A web-based interface built using React.js and Web3.js enables secure interaction with the blockchain, while wallet-based authentication ensures that each authorized user can cast only one vote The system is implemented and tested in a controlled environment to evaluate performance, accuracy, and resistance to double voting.***

Keywords: Blockchain, Ethereum, Smart Contracts, Decentralized Voting, Digital Elections, Secure Authentication, Immutable Ledger.

I. INTRODUCTION

In democratic societies, elections serve as the foundation for selecting representatives and shaping public governance. However, traditional paper-based voting systems and centralized electronic voting mechanisms often face issues such as limited transparency, susceptibility to manipulation, delayed result processing, and reliance on centralized authorities. These challenges can reduce public trust and raise concerns about election integrity and data security.

Advancements in blockchain technology have introduced new possibilities for designing secure and tamper-resistant digital voting platforms. Blockchain provides a decentralized and immutable ledger where transactions are recorded across multiple network nodes, making unauthorized modifications computationally impractical. Smart contracts enable automated enforcement of election rules such as voter registration, vote validation, and result computation without requiring continuous human supervision.

This project presents a Blockchain-Based Voting System developed on the Ethereum platform. The system utilizes Solidity smart contracts to manage election logic and record votes as immutable blockchain transactions. A web-based interface built using React.js and Web3.js enables secure interaction with the blockchain, while MetaMask authentication ensures that only authorized users can cast a single vote. The system is developed and tested in a controlled environment to evaluate functionality, transparency, and resistance to double voting. By integrating decentralized validation with automated smart contract execution, the proposed framework aims to enhance security, auditability, and trust in digital electoral processes.

TABLE I
COMPARISON OF VOTING APPROACHES

Feature	Traditional Paper Voting	Electronic Voting Machines (EVM)	Blockchain-Based Voting
Control Mechanism	Manual supervision	Centralized authority control	Decentralized consensus mechanism
Transparency	Limited	Moderate	High (public ledger verification)
Tamper Resistance	Low	Moderate	High (immutable blockchain records)
Single Point of Failure	No	Yes	No
Vote Counting	Manual counting	Electronic counting	Smart contract-based automatic counting
Auditability	Time-consuming and physical verification	Authority-dependent verification	Cryptographically verifiable and transparent
Data Storage	Physical ballot storage	Centralized database or hardware	Distributed ledger across nodes
Security Level	Procedural security	Hardware and software security	Cryptographic and consensus-based security

©IJRASET: All Rights are Reserved

II. LITERATURE REVIEW

Blockchain technology was first introduced in [1] as a decentralized and immutable transaction ledger designed to eliminate the need for trusted intermediaries. The concept established the foundation for secure and tamper-resistant distributed systems. Later, [2] introduced the Ethereum platform, which extended blockchain capabilities by enabling programmable smart contracts for decentralized applications. These advancements laid the groundwork for blockchain-based electronic governance systems.

A comprehensive overview of blockchain architecture, consensus mechanisms, and security features was presented in [3]. The study discussed decentralization, immutability, and transparency as key properties that make blockchain suitable for applications requiring high integrity and trust, including digital voting systems.

In [4], the authors proposed a blockchain-based electronic voting framework to improve transparency and reliability. The study demonstrated how blockchain can enhance auditability and reduce election fraud risks. However, scalability and transaction efficiency were identified as challenges for large-scale deployment.

The work in [5] reviewed blockchain-based electronic voting systems and highlighted open research challenges related to privacy preservation, voter authentication, and system scalability. The study emphasized the need for balancing transparency with confidentiality in digital elections.

A large-scale blockchain-based e-voting architecture using hybrid consensus and sharding techniques was presented in [6]. The proposed model aimed to enhance transaction throughput and reduce latency, making blockchain voting more suitable for national-level elections.

In [7], a self-tallying voting protocol integrated with blockchain was introduced to ensure privacy and verifiability. The protocol enabled voters to verify results without revealing individual voting choices, thereby strengthening election integrity.

The integration of biometric authentication with blockchain-based voting was explored in [8]. The study demonstrated how biometric verification can enhance voter identity validation while maintaining decentralized record storage.

An Ethereum-based electronic voting system was proposed in [9], where smart contracts were used to automate vote recording and counting. The implementation demonstrated improved transparency and tamper resistance compared to centralized systems.

Additionally, [10] introduced an anti-quantum secure voting protocol integrated with blockchain to enhance cryptographic security against emerging computational threats, further strengthening the reliability of decentralized voting mechanisms.

Building upon these studies, the present work implements a decentralized voting framework using Ethereum smart contracts and a web-based interface to ensure secure vote casting, transparent result computation, and resistance to double voting. The system is developed and evaluated in a controlled environment to validate performance, integrity, and operational reliability.

III.SYSTEM ARCHITECTURE AND METHODOLOGY

A. *System Overview*

The proposed Blockchain-Based Voting System is implemented as a decentralized web-based application designed to ensure secure, transparent, and tamper-resistant digital elections. The system integrates Ethereum blockchain technology with a user-friendly web interface to facilitate secure voter participation and automated election management.

The overall architecture follows a modular layered design consisting of the following core components:

1) Frontend Interface for voter and administrator interaction
2) Blockchain Interaction Module for communication with the Ethereum network
3) Smart Contract Layer for enforcing election rules and vote management
4) Identity and Wallet Management Module for secure authentication and transaction authorization

The data flow begins with user interaction at the frontend layer, followed by transaction processing through Web3.js, execution of election logic within smart contracts, and permanent storage of votes on the blockchain ledger. This modular architecture ensures scalability, security, maintainability, and clear separation of system responsibilities.

B. *Overview of Blockchain Technology*

Blockchain is a distributed digital ledger technology that stores data in a decentralized and immutable manner. Instead of relying on a centralized database, blockchain distributes records across multiple nodes within a peer-to-peer network. Data is stored in blocks, where each block contains transaction details, a timestamp, and a cryptographic hash of the previous block. This chaining mechanism ensures data integrity and prevents unauthorized modifications.

Key features of blockchain that make it suitable for voting systems include decentralization, immutability, transparency, and cryptographic security.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Once a vote is recorded as a transaction and confirmed through a consensus mechanism, it cannot be altered or deleted. The distributed structure eliminates single points of failure, reducing the risk of manipulation and cyberattacks. These characteristics make blockchain an effective platform for secure electronic voting.

C. System Architecture

The proposed system adopts a layered architectural approach to enhance modularity and reliability. Each layer performs a specific function within the voting process:

1) *Frontend Layer:* Provides an intuitive interface for voter registration, vote casting, and result viewing, as well as administrative controls for election management.
2) *Blockchain Interaction Layer:* Acts as a bridge between the user interface and the Ethereum blockchain using Web3.js
3) *Smart Contract Layer:* Implements election logic, vote validation, and rule enforcement.
4) *Development and Testing Environment:* Supports deployment and simulation of the blockchain network.

This structured design ensures secure communication between components while isolating critical blockchain logic from user interface operations.

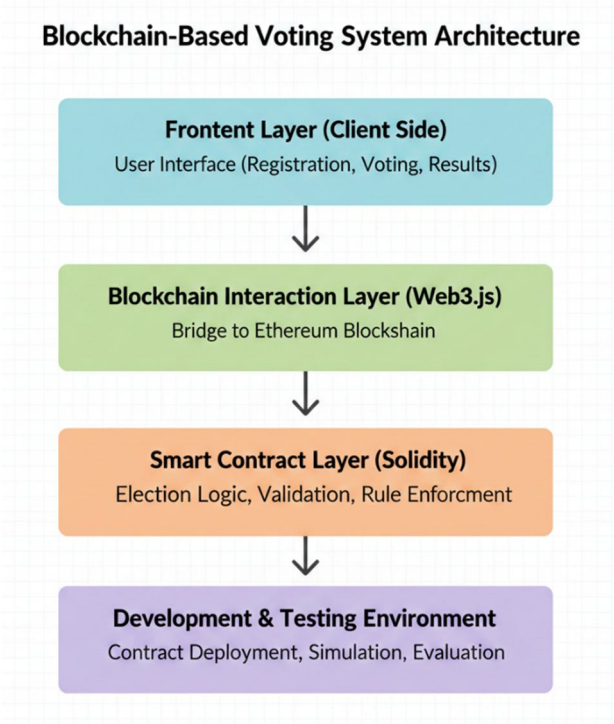


Fig. 1: Layered Architecture of the Blockchain-Based Voting System

D. Frontend Layer (Client Side)

The frontend layer is developed using React.js along with JavaScript (ES6), HTML5, and CSS3 to create a responsive and user-friendly interface. React Router DOM is used to manage navigation between application pages.

This layer enables voters to register, authenticate, and cast votes securely. It also provides administrative functionalities such as candidate addition, election initialization, and result declaration. The frontend communicates with the blockchain via Web3.js to enable real-time interaction with deployed smart contracts.

E. Blockchain Interaction Layer

The Blockchain Interaction Layer facilitates communication between the frontend application and the Ethereum blockchain. It is implemented using Web3.js, which enables reading from and writing to smart contracts deployed on the Ethereum network.

Through this module, the system retrieves election data such as candidate details, voting status, and vote counts. It also submits transactions for voter registration and vote casting. Web3.js ensures secure and reliable blockchain communication while maintaining compatibility with Ethereum development tools.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

F. Smart Contract Layer

The Smart Contract Layer forms the core logic of the voting system and is implemented using Solidity (version 0.5.16) on the Ethereum Virtual Machine (EVM).

The primary Election smart contract enforces critical election rules, including:

1) One-vote-per-voter policy
2) Voter eligibility verification
3) Candidate management
4) Secure vote recording
5) Automated vote counting

Once deployed, the smart contract operates autonomously, ensuring that all election processes are executed transparently and without manual intervention. Since smart contracts are immutable after deployment, they prevent unauthorized modifications to election logic.

G. Blockchain Development and Testing Environment

The system is developed and tested using the Truffle Framework, which provides tools for compiling, deploying, and managing smart contracts. A local blockchain network is simulated using Ganache CLI, enabling safe and cost-free experimentation.

Ganache provides multiple test accounts with preloaded Ether, allowing developers to test transactions, measure gas consumption, and evaluate system performance before deployment to a live network. Migration scripts ensure controlled and consistent contract deployment across development stages.

H. Wallet and Identity Management

User authentication and transaction authorization are handled using MetaMask, a browser-based Ethereum wallet. MetaMask enables secure account management and digital signature verification for blockchain transactions.

In the proposed system, MetaMask ensures that only authorized voters can cast votes. Each voting transaction must be explicitly approved by the user, enhancing transparency and preventing unauthorized activity. This cryptographic identity management mechanism strengthens election integrity while preserving voter anonymity.

I. Build and Package Management

The system utilizes Node.js and npm for dependency management and build configuration. These tools manage required libraries, execute scripts, and support both frontend and blockchain services. The modular code structure enhances maintainability and allows future upgrades without disrupting existing functionality.

IV. RESULTS AND ANALYSIS

The Blockchain-Based Voting System was evaluated through functional testing and scenario-based validation to assess its performance, accuracy, and reliability in a simulated election environment. A controlled user dataset was created to simulate voter registration, authentication, vote casting, and result computation. The system was tested across its core modules, including voter verification, smart contract execution on the blockchain network, automated vote recording, and decentralized storage mechanisms.

The results demonstrate the system's ability to provide a secure, transparent, and efficient voting process. By replicating real-time election scenarios, the testing environment enabled validation of system integrity, rule enforcement, and automated result generation. The following key outcomes were observed during system evaluation:

1) *Accurate Voter Authentication:* The voter verification mechanism successfully authenticated eligible users and prevented unauthorized access. The system ensured that only registered voters could participate in the election process while maintaining privacy throughout the workflow.
2) *Secure and Immutable Vote Recording:* Votes submitted through the decentralized application were permanently recorded on the blockchain network. Smart contracts strictly enforced the "one person, one vote" rule and automatically rejected duplicate voting attempts. Once recorded, votes could not be altered or removed.
3) *Tamper-Resistant Data Storage:* Election-related data such as candidate details and voting logs were securely stored using decentralized storage. The reference identifiers were recorded on-chain, ensuring data verification without enabling modification, thereby supporting full auditability.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

4) *Real-Time Vote Tallying:* The smart contract automatically updated vote counts as transactions were confirmed. Results were displayed instantly on the administrative dashboard without manual intervention, eliminating counting errors and ensuring transparency.
5) *Administrative Monitoring and Control:* Election administrators were able to manage the entire election lifecycle, including adding candidates, starting and ending elections, and monitoring system activity. The structured dashboard ensured controlled access and accountability for administrative actions.
6) *Scalability and Performance Efficiency:* The blockchain-based infrastructure supported reliable transaction processing with optimized network performance. The system demonstrated suitability for institutional, organizational, and campus-level deployments while maintaining operational stability.

These results confirm the effectiveness of the proposed system in delivering a secure, transparent, and reliable blockchain-enabled voting platform. The integration of decentralized record management and automated contract execution establishes this system as a strong alternative to conventional digital voting methods.

Fig. 2. Landing Page

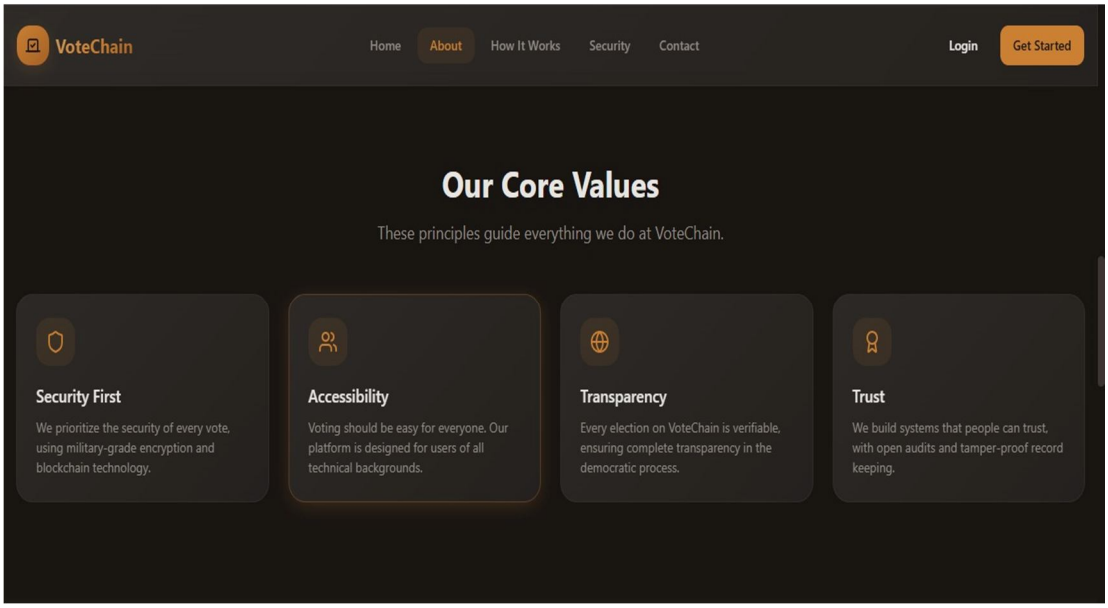


Fig. 3. Home Page

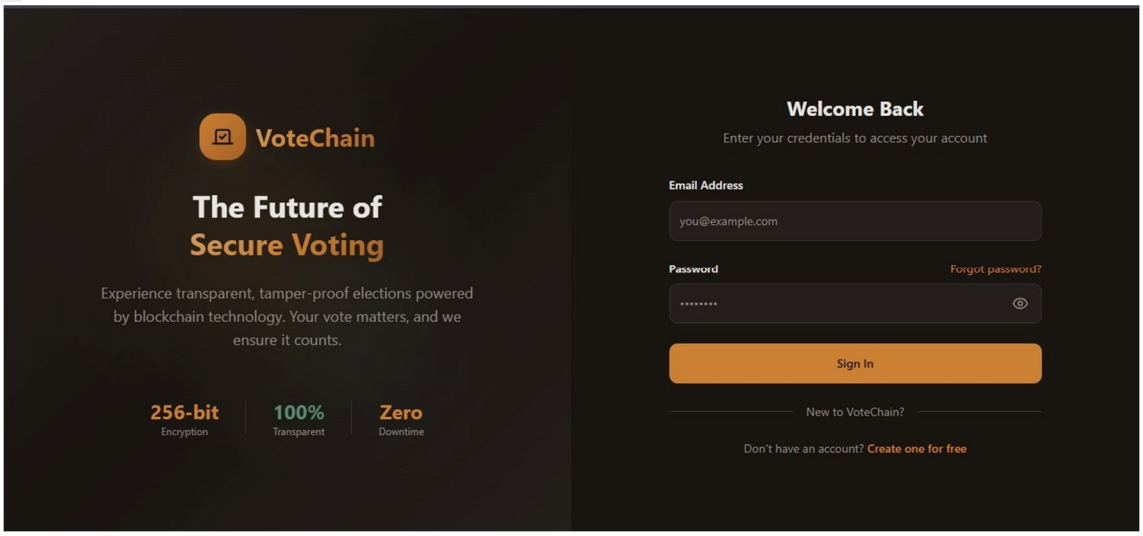


Fig. 4. Login Page

V. CONCLUSION

The Blockchain-Based Voting System presented in this work demonstrates the effectiveness of integrating decentralized technologies and structured authentication mechanisms to modernize the electoral process. Unlike traditional voting systems, the proposed architecture ensures transparency, immutability, and privacy through blockchain-based record management and decentralized storage mechanisms.

The system enables secure voter registration through OTP-based verification, automated vote recording through smart contracts, and real-time result computation without manual intervention. Each vote is permanently stored on the blockchain ledger, preventing modification or deletion after confirmation. The enforcement of the one-vote-per-voter rule ensures fairness and integrity throughout the election lifecycle.

Experimental evaluation confirmed accurate vote handling, prevention of duplicate voting, tamper resistance, and smooth system operation. The modular layered architecture enhances maintainability and supports scalability for institutional and large-scale election environments. By eliminating centralized control points and reducing manual dependency, the system strengthens electoral trust and minimizes fraud risks.

Overall, this work validates blockchain technology as a reliable framework for secure, transparent, and efficient digital voting systems, providing a foundation for future advancements in electronic governance.

VI. FUTURE WORK

Future enhancements will focus on improving usability, efficiency, and scalability while remaining within the same application domain. Although the proposed system demonstrates strong security and transparency, further improvements can strengthen its performance for large-scale real-world deployment.

The blockchain framework can be optimized to support higher transaction throughput, enabling the system to efficiently handle large-scale elections with increased voter participation. Optimization of block generation time and validation mechanisms can further enhance system responsiveness and reduce processing delays during peak voting periods. Stronger voter authentication mechanisms may also be integrated to improve eligibility verification and reinforce election integrity.

Advanced blockchain validation techniques can be implemented to strengthen tamper detection and improve audit capabilities. Additionally, optimizing the voting interface for both web and mobile platforms will improve accessibility and encourage wider public participation. These improvements will move the proposed blockchain-based voting system closer to practical deployment in secure, transparent, and real-world election environments.

VII. ACKNOWLEDGEMENT

We would like to express our sincere gratitude to everyone who contributed directly or indirectly to the successful completion of this project. We are thankful to the Department of Computer Engineering, V.E.S. Polytechnic, Mumbai, for providing the necessary academic resources, technical guidance, and a supportive learning environment.

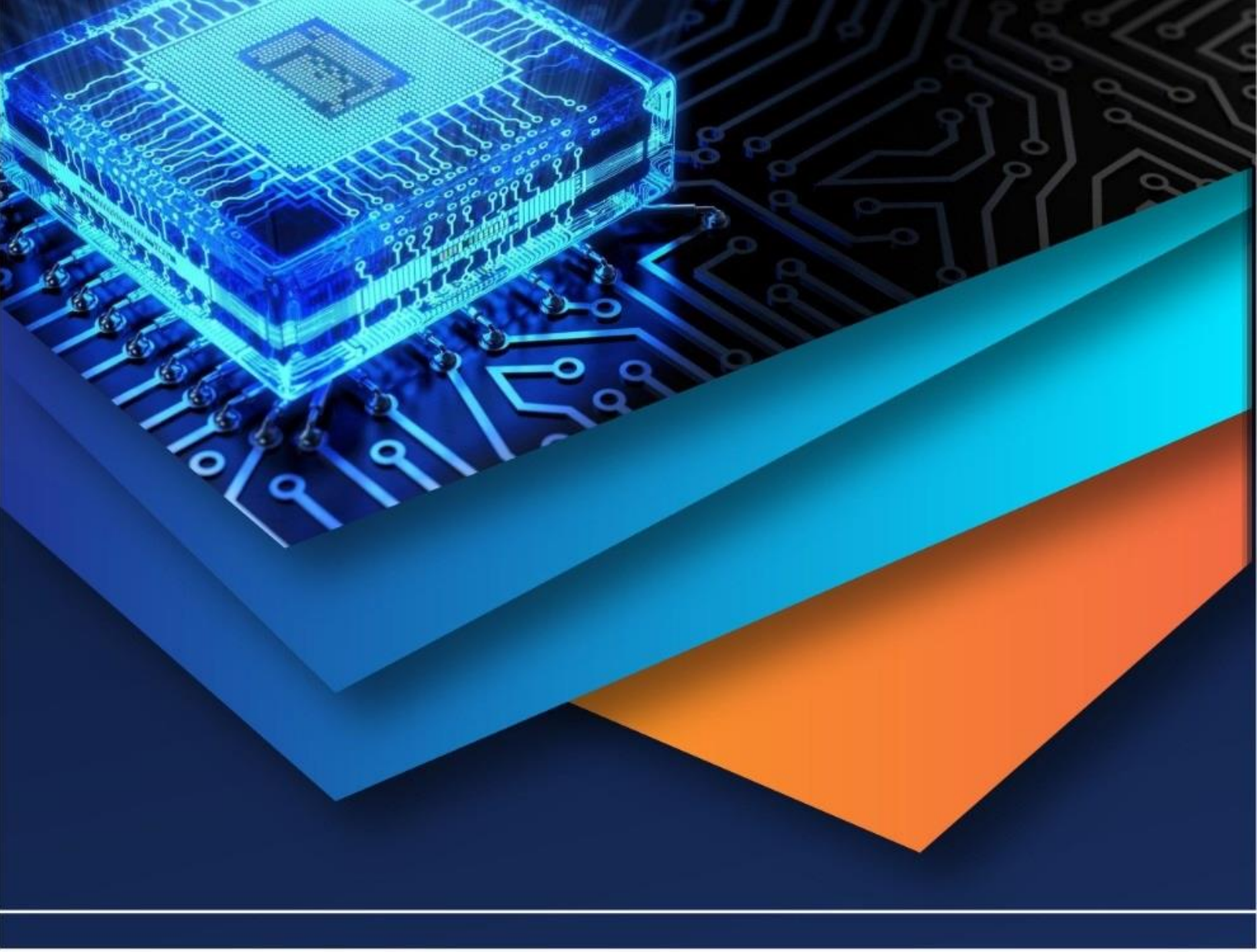
©IJRASET: All Rights are Reserved

We also extend our appreciation to the faculty members, staff, classmates, friends, and family members whose encouragement and assistance played an important role throughout the development of this project. Their continuous support and motivation helped us overcome challenges and successfully accomplish our objectives.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014. [Online]. Available: https://ethereum.org
[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in Proc. IEEE Int. Congress on Big Data (BigData Congress), 2017, pp. 557–564.
[4] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," IEEE Access, vol. 7, pp. 24477–24488, 2019.
[5] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—Review and open research challenges," Sensors, vol. 21, no. 17, pp. 1–30, 2021.
[6] Y. Abuidris et al., "Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding," ETRI Journal, vol. 43, no. 2, pp. 357–370, Apr. 2021.
[7] X. Xia and J. Zhou, "A self-tallying voting protocol with blockchain," IEEE Transactions on Information Forensics and Security, vol. 16, pp. 477–491, 2021.
[8] M. J. M. Chowdhury et al., "Blockchain-based biometric voting system," Journal of Network and Computer Applications, vol. 190, p. 103124, 2021.
[9] A. R. Khan, M. M. Khan, and A. Rehman, "Blockchain-based e-voting system using Ethereum," International Journal of Advanced Computer Science and Applications, vol. 11, no. 10, pp. 190–196, 2020.
[10] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," IEEE Access, vol. 7, pp. 115304–115316, 2019.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)