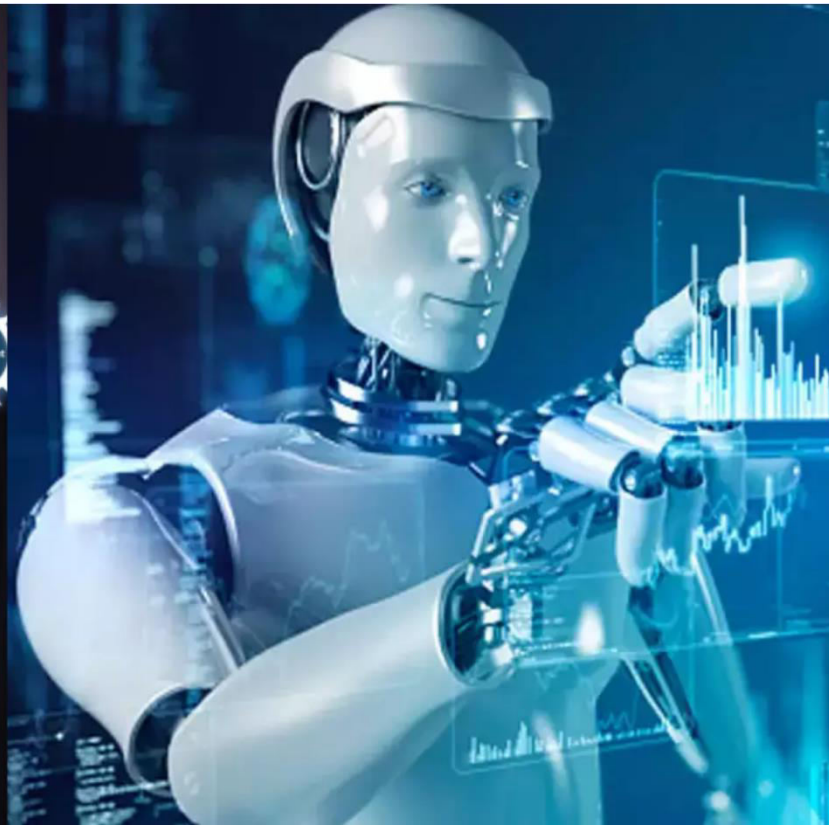
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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

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



Impact Factor: 8.699

Volume 15, Special Issue 1, January 2026

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

Transparent and Secure E-Voting using Block chain

Prof. Megha Joshi[1], Aditya Raste[2], Purva Savale[3], Tanmay Auti[4], Shweta Kamble[5]

Professor, Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[1]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[2]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[3]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[4]

Dept. of CE, Indala College of Engineering, Kalyan, Maharashtra, India[5]

ABSTRACT: Democratic voting serves as a fundamental pillar of modern society, yet traditional paper-based or centralized electronic voting systems often face challenges regarding transparency, security, and public trust. Centralized databases are vulnerable to data tampering, unauthorized access, and manipulation, which can compromise the integrity of an election. This paper reviews a transparent and secure E-Voting system designed to overcome these limitations by leveraging Blockchain technology. The proposed system utilizes a decentralized and distributed ledger framework to ensure that voting records are immutable and publicly verifiable without compromising voter privacy.

The system employs smart contracts to automate the voting process, ensuring that valid votes are counted accurately and eliminating the need for a central trusted authority. Cryptographic hashing techniques (such as SHA-256) are used to secure voter data and link blocks, making the chain tamper-proof. Experimental analysis demonstrates that this blockchain-based approach significantly enhances security against fraud, prevents double-voting, and provides a fully auditable trail of all transactions. The presented framework offers a robust, cost-effective, and highly accessible solution that restores trust in the electoral process.

KEYWORDS: E-Voting, Blockchain Technology, Smart Contracts, Decentralization, Cryptography, Distributed Ledger Technology (DLT), Data Integrity, Security, Transparency, SHA-256, Ethereum.

I. INTRODUCTION

Democratic elections are the primary medium for citizens to express their will, yet many existing systems suffer from a lack of transparency and security. Traditional paper ballots are prone to physical tampering and counting errors, while centralized Electronic Voting Machines (EVMs) often face skepticism regarding software manipulation and lack of auditability. This "trust gap" often discourages voter participation and leads to disputes over election results.

Automated E-Voting systems aim to reduce these barriers by digitizing the process, but centralized servers remain a single point of failure. However, implementing a truly secure system is challenging due to threats such as hacking, identity theft, and administrative fraud. Traditional database-driven approaches typically fail to provide guaranteed immutability, as database administrators theoretically retain the power to alter records. The reviewed system focuses on conducting elections using a decentralized Blockchain network, a method that is hardware-independent on the user side but cryptographically secure on the backend. Smart Contracts are used to govern the election rules, ensuring that once a vote is cast, it is permanently recorded on the blockchain ledger. The voting data is protected using cryptographic hashing, ensuring that any attempt to alter a past vote would invalidate the entire chain. This paper reviews the system's architecture, transaction validation pipeline, security strategy, and overall performance, demonstrating that reliable, transparent, and tamper-proof elections can be achieved using accessible Blockchain technologies.

II. SYSTEM ARCHITECTURE FOR ROBUST SECURITY

Reliable election management begins with a secure and decentralized infrastructure. The reviewed system adopts a distributed network design that emphasizes data integrity, voter authentication, and immutable record-keeping to ensure accurate results under varied conditions.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

2.1 Frontend Interface and Voter Authentication

The system uses a standard web-based interface (Web3) as the primary input device, making it widely accessible via smartphones or computers without requiring specialized voting hardware. The interface connects to a digital wallet (e.g., MetaMask) to authenticate the user's identity. This approach ensures that users can vote remotely while maintaining strict access control.

2.2 Distributed Ledger Framework

To handle security risks such as server hacking or data manipulation, the system integrates a decentralized Blockchain framework (such as Ethereum or Hyperledger). The Blockchain serves as a digital ledger where every vote is recorded as a transaction. Unlike centralized servers where data is stored in one location, the ledger is replicated across multiple nodes in the network. This distribution ensures that even if one node is compromised, the integrity of the election remains intact, improving system reliability.

2.3 Smart Contract Logic

The system utilizes Smart Contracts—self-executing code stored on the blockchain—to automate the election process. These contracts define the rules of the election (e.g., voting duration, candidate list, one-vote-per-person). This removes the need for human intervention during the counting process and ensures that the rules are enforced strictly by the code.

III. GESTURE PROCESSING AND CLASSIFICATION PIPELINE

Once the voter submits their choice, the data proceeds through a structured pipeline designed to accurately validate and record the vote. Each stage of the pipeline ensures that the vote is legitimate while maintaining voter anonymity.

3.1 Voter Eligibility and Double-Voting Prevention

Allowing invalid or duplicate votes is a major flaw in traditional systems. Instead of manual checking, the Smart Contract checks the voter's digital address against the registered voter roll. If the address has already cast a vote, the transaction is rejected immediately. This prevents double-voting and ensures that only eligible participants can influence the outcome.

3.2 Challenges in Centralized Database Voting

Traditional SQL-based voting systems rely heavily on central administrators to secure the database. In real-world scenarios, these systems are vulnerable to "SQL Injection" attacks, insider threats, or accidental data loss. Such vulnerabilities make centralized systems unreliable for high-stakes elections, where a single altered record can change the outcome. For this reason, the system avoids mutable database storage for the actual vote records.

3.3 Block Creation and Hashing

Instead of updating a table row, the system bundles votes into "blocks." Each block contains a cryptographic hash of the previous block, creating a linked chain. This method retains the essential history of the election. The hashing mechanism offers several advantages: it makes the data tamper-evident (changing one vote changes the hash), reduces reliance on trust, and provides a permanent audit trail. This structure is particularly effective for elections, where the sequence and integrity of votes are critical.

IV. RESULT GENERATION AND AUDITABILITY

Once the vote has been validated and added to the blockchain, the system focuses on producing clear and verifiable election results. This stage involves querying the ledger to tally votes and allowing public verification.

4.1 Real-Time Tallying

Election results usually take hours or days to count in traditional systems. To prevent delays and uncertainty, the system allows for real-time tallying. Since every vote is a confirmed transaction on the ledger, the current count can be calculated instantly by querying the smart contract. This mechanism ensures that the results are available immediately after the election closes.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

International Conference on Emerging Technologies and Pharmaceutical Research (ICETPR 2026)

17–18 January 2026

Indala College of Engineering, Polytechnic & Pharmacy, Kalyan, MH, India

|Volume 15, Special Issue 1, January 2026|

4.2 Public Verification and Transparency

Individual voters can verify that their vote was counted. The system provides a transaction ID (hash) to the voter. Using this ID, the voter can look up their transaction on the public ledger to confirm it was included in a block. This method empowers voters to audit the system personally, fostering trust in the democratic process.

4.3 Modular Expansion for Future Features

The design of the blockchain module allows for easy future expansion. Potential enhancements include biometric integration for tighter security, multi-constituency support, and hybrid voting models (combining physical booths with blockchain backends). This modular framework ensures that the system remains scalable as blockchain technology matures.

V. CONCLUSION

This paper reviewed a system designed to conduct transparent and secure elections using blockchain technology and smart contracts. by combining a web3 frontend, decentralized ledger storage, and cryptographic hashing, the system achieves robust security without relying on a central authority. the use of immutable blocks effectively minimizes the impact of external hacking, insider fraud, and data tampering, resulting in high integrity for the electoral process. the modular integration of voter authentication, smart contract automation, and public auditability enables seamless trust between the government and citizens, offering a practical solution for modern democracy. as the system continues to evolve, future enhancements may include mobile-app integration, government id api linking, and zero-knowledge proofs for enhanced privacy. overall, this framework demonstrates that efficient and secure e-voting is achievable on standard computing platforms, making it a promising contribution to digital governance

REFERENCES

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Decentralized Business Review, 2008.
2. Buterin, “A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2014.
3. F. P. Hjalmarsson, G. K. Hreidarsson, M. M. Hamdaqa, and G. Hjalmtysson, “Blockchain-Based E-Voting System,” Proc. IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983–986, 2018.
4. K. M. Khan, J. Arshad, and M. M. Khan, “Secure Digital Voting System based on Blockchain Technology,” International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, 2018.
5. N. Kshetri and J. Voas, “Blockchain-Enabled E-Voting,” IEEE Software, vol. 35, no. 4, pp. 95–99, 2018.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details