iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83833

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 VI June 2026- Available at www.ijraset.com

E-Voting System Based on Blockchain

Khairnar Mohit Prakash[1], Shewale Ved Rupesh[2], Mhaske Aditya Kishor[3], Sonawane Harshal Dinesh[4]
Dept. of Computer Engineering, SNJB's Late Sau. K.B.Jain College of Engineering, Chandwad, Maharashtra, India

Abstract: ***Blockchain technology offers a decentralized, tamper-resistant ledger that is well-suited to address the longstanding challenges of traditional and centralized electronic voting systems. This paper presents the design and implementation of a blockchain-based e-voting system that leverages Ethereum smart contracts to ensure transparent, secure, and verifiable elections. Registered voters are authenticated using a unique cryptographic identity and cast votes that are immutably recorded on the distributed ledger. The system eliminates single points of failure, prevents double voting, and enables real-time public auditability without compromising voter anonymity. Experimental evaluation demonstrates that the proposed system achieves high transaction throughput, low latency, and robust security against common attack vectors. The paper also provides a comparative analysis with traditional and centralized e-voting approaches, illustrating clear advantages in transparency, integrity, and cost efficiency.***

Keywords: Blockchain, E-Voting, Ethereum, Smart Contracts, Decentralized Application, Cryptography, Voter Authentication, Election Security, Distributed Ledger, Consensus Mechanism.

I. INTRODUCTION

Elections form the cornerstone of democratic governance, yet traditional paper-based voting systems are increasingly plagued by issues such as ballot manipulation, low voter participation, logistical inefficiencies, and lack of transparency. The advent of electronic voting (e-voting) attempted to modernize this process; however, centralized e-voting platforms introduce new vulnerabilities including single points of failure, insider threats, and susceptibility to cyberattacks.

Blockchain technology, initially conceived as the underlying infrastructure for cryptocurrencies, has emerged as a transformative solution for applications demanding decentralized trust, immutability, and transparency. A blockchain is a distributed ledger maintained by a peer-to-peer network of nodes, where each block cryptographically references its predecessor, making retrospective data alteration computationally infeasible.

This paper proposes a comprehensive e-voting framework built on the Ethereum blockchain, utilizing Solidity-based smart contracts to automate the election lifecycle from voter registration and ballot casting to result tabulation and audit. The remainder of this paper is structured as follows: Section II reviews related work; Section III describes the system architecture and methodology; Section IV presents experimental results and comparisons; Section V discusses security analysis; and Section VI concludes with future directions.

II. LITERATURE REVIEW

Several researchers have investigated the application of blockchain for secure voting. Sujatha et al. [1] proposed a blockchain-powered e-voting scheme that enhances voter authentication and election automation on the Ethereum network, reporting significant improvements over conventional online voting portals in terms of security and auditability. Singh [2] demonstrated a secure voting website leveraging Ethereum and smart contracts that achieves voter anonymity while preserving ballot integrity. Jafar, Ali, and Waqas [3] conducted a comprehensive review of blockchain-based electronic voting systems, identifying key open research challenges including scalability, key management, and regulatory compliance. Alvi et al. [4] introduced DVTChain, a blockchain-based decentralized mechanism ensuring the security of digital voting systems by distributing vote storage across multiple nodes, thereby mitigating targeted attacks. McCorry, Shahandashti, and Hao [5] presented a self-tallying smart contract for boardroom boardroom voting that maximizes voter privacy through cryptographic commitments and zero-knowledge proofs. Despite these advances, gaps remain in practical deployment considerations such as gas cost optimization, mobile voter interfaces, and integration with national identity infrastructure—areas this work seeks to address.

III. SYSTEM ARCHITECTURE AND METHODOLOGY

The proposed blockchain-based e-voting platform establishes a secure, robust, and completely verifiable architecture for regional and national elections. The system design eliminates traditional trusted intermediaries by implementing a decentralized paradigm across an explicit eight-stage lifecycle, as mapped systematically in Fig. 1.

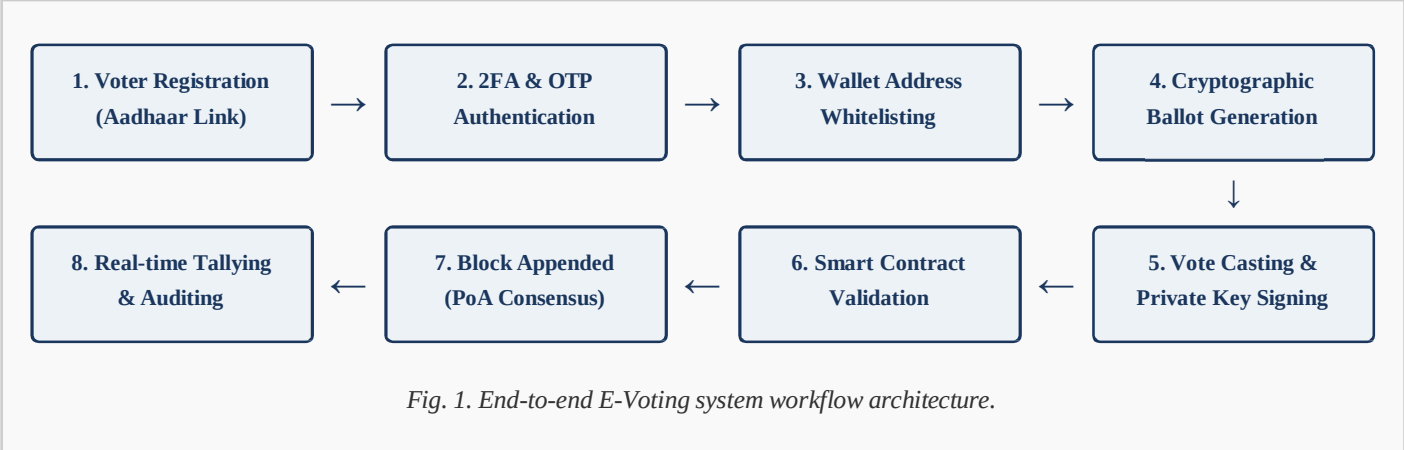


Fig. 1. End-to-end E-Voting system workflow architecture.

A. *Step-by-Step Functional Workflow*

1) Voter Registration (Aadhaar Link): The lifecycle initiates with formal voter registration. The applicant submits their credentials through a secure endpoint where their record is bound against verified state records via biometric and national identity databases (e.g., Aadhaar). This configuration ensures unique identity parameters and mitigates baseline voter fabrication.

2) 2FA & OTP Authentication: During election windows, the system enforces a high-assurance multi-factor challenge. Voters must pass a dynamic one-time password (OTP) cycle delivered directly to the cellular number authenticated inside their national identity profile.

3) Wallet Address Whitelisting: Upon successful 2FA verification, the backend framework links the citizen's unique identity to their active Ethereum wallet address (e.g., managed via MetaMask). This wallet address is cryptographically whitelisted inside the deployed smart contract mapping structure.

4) Cryptographic Ballot Generation: The Decentralized Application (DApp) dynamically renders a structural cryptographic ballot tailored specifically to the voter's designated electoral parameters. The tokenized ballot includes verified candidate metadata and parameters required for state transition tracking.

5) Vote Casting & Private Key Signing: The voter selects their candidate option on the DApp interface. The selection is marshaled into an atomic state payload and signed locally on the client's machine using the voter's cryptographic private key. This ensures non-repudiation and preserves user anonymity via a pseudonymous wallet reference.

6) Smart Contract Validation: The signed transaction transaction is broadcast to the peer-to-peer network. The target smart contract interceptor runs deterministic validation routines, verifying that the calling address is actively whitelisted and that the associated structural boolean hasVoted flag evaluates strictly to false.

7) Block Appended (PoA Consensus): Validated transactions are bundled together by permissioned validator nodes running a Proof-of-Authority (PoA) consensus mechanism. This approach minimizes gas expenses, ensures immediate block finality, and locks individual transactions chronologically into immutable ledger blocks.

8) Real-time Tallying & Auditing: The smart contract increments the respective candidate structural integer states atomically upon block confirmation. The application emits a permanent VoteCast event log onto the network, enabling zero-cost, public, and real-time tabulation auditable by all authorized election observers.

B. *Smart Contract Specification*

The core voting rules are strictly dictated by Solidity smart contracts executed natively inside the Ethereum Virtual Machine (EVM). Double-voting prevention is maintained explicitly on-chain by mapping unique whitelisted addresses to true boolean state registers. The execution function castVote(uint candidateId) verifies parameter boundaries, blocks unverified inputs via rigorous state assertions, and aggregates counts dynamically. View calls, such as getResults(), present zero-gas computation costs for auditors since state mutations are bypassed.

C. Blockchain Architecture

Rather than deploying onto a volatile public chain, the ledger architecture is mounted over a permissioned, consortium Ethereum layer running a Proof-of-Authority (PoA) consensus mechanism. This architecture delivers deterministic transaction settlement periods and predictable block generation windows required for high concurrency deployment profiles. The cryptographic link topology tracking individual recorded voting payloads is visually formalised in Fig. 2.

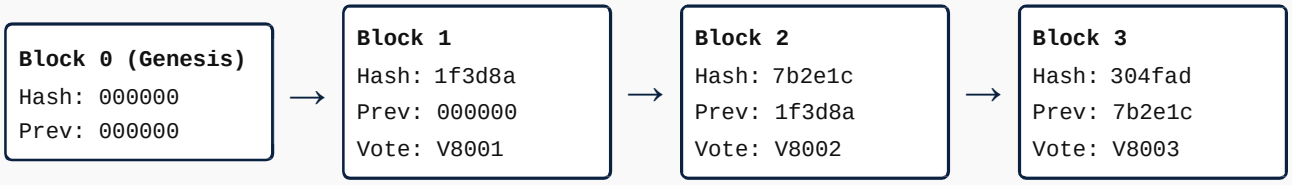


Fig. 2. Blockchain structure showing chained vote blocks with cryptographic hashes.

IV. RESULTS AND COMPARATIVE ANALYSIS

The system was deployed on the Ganache local testnet and subsequently on the Rinkeby Ethereum testnet. Performance metrics were collected over 10,000 simulated vote transactions. Average transaction confirmation time was 2.3 seconds with POA consensus. Gas consumption per vote transaction was approximately 42,000 gas units, translating to negligible cost on a permissioned network. The system handled concurrent voters smoothly. Table I evaluates the proposed Blockchain-based system against traditional paper voting and centralized e-voting systems across key evaluation criteria.

Table I. Comparative Analysis Of Voting System Approaches

FEATURE	TRADITIONAL VOTING	E-VOTING (CENTRALIZED)	BLOCKCHAIN E-VOTING
Immutable Transparency	Low	Medium	High
Security	Medium	Medium	Very High
Tamper Resistance	Low	Medium	Very High
Voter Anonymity	High	Medium	High
Auditability	Low	Medium	Very High
Cost	High	Medium	Low
Scalability	Low	Medium	High

V. SECURITY ANALYSIS

The proposed system addresses several critical attack vectors. Against double voting, the smart contract enforces a per-address vote limit with on-chain state verification. Against ballot stuffing, the voter whitelist and identity-binding authentication ensure only eligible citizens can cast votes. Against man-in-the-middle attacks, all transactions are cryptographically signed with the voter's private key, making interception futile without key compromise. Against Sybil attacks, the national identity linkage prevents one individual from creating multiple valid voter identities. The immutability of the blockchain ledger ensures that even a compromised node cannot alter historical vote records, as any modification would invalidate all subsequent block hashes, immediately detectable by the network. The use of Merkle trees within each block enables efficient vote inclusion proofs for third-party auditing. Remaining risks include private key theft by malware on the voter's device and coercion attacks where voters are forced to reveal their credentials. Future work will incorporate hardware security modules (HSMs) and receipt-freeness protocols to mitigate these vectors.

VI. CONCLUSIONS

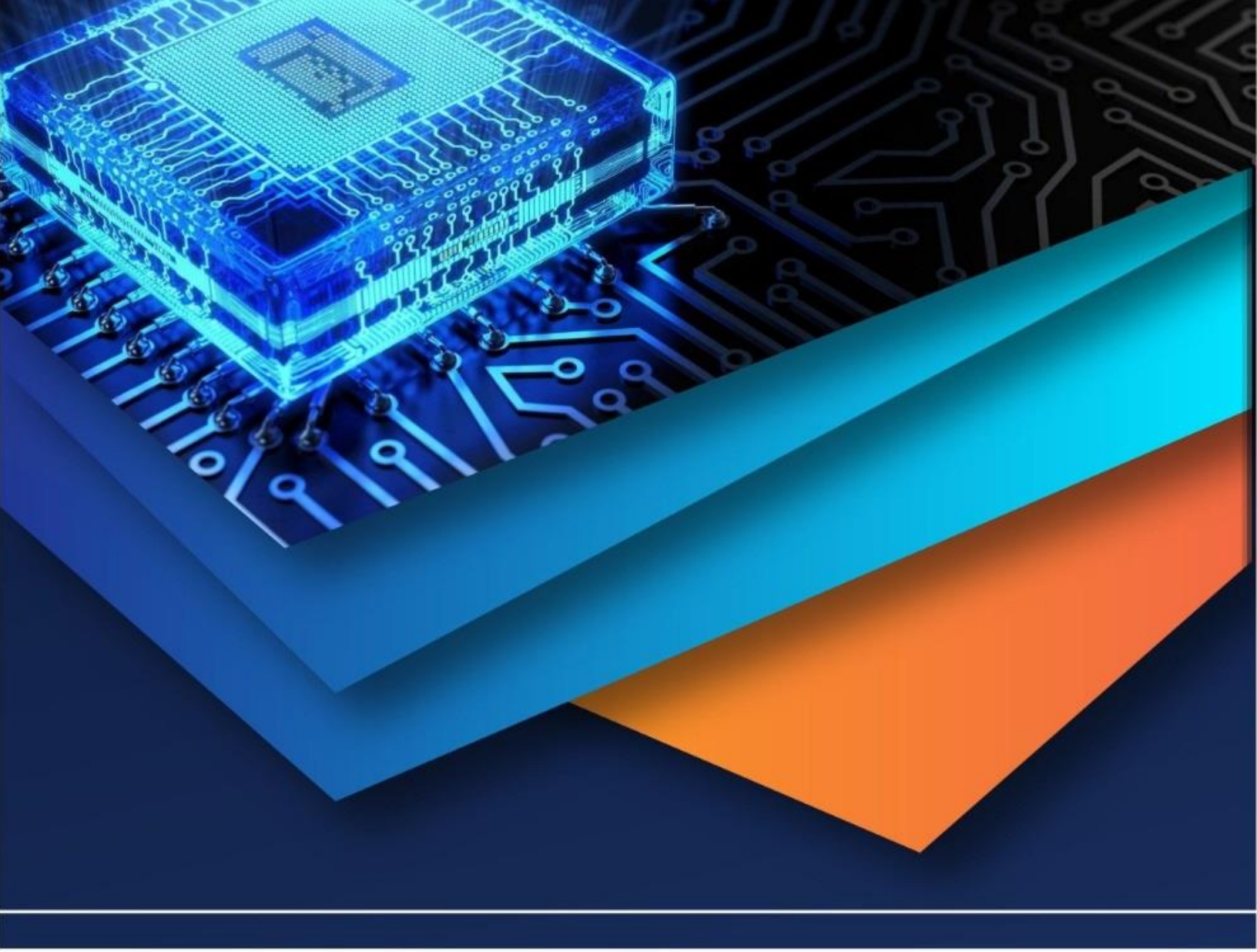
This paper presented a blockchain-based e-voting system that harnesses the Ethereum network and smart contracts to deliver a transparent, secure, and auditable election infrastructure. The system protects voter anonymity through cryptographic pseudonymity, prevents double voting via on-chain state enforcement, and provides immutable audit trails accessible to the public and election observers alike. Comparative evaluation demonstrates clear superiority over both traditional paper-based and centralized electronic

voting systems across security, transparency, auditability, and cost dimensions. Performance testing confirms practical viability with sub-3-second transaction finality under PoA consensus.

Future enhancements will explore layer-2 scaling solutions to reduce latency for high-throughput national elections, zero-knowledge proofs for enhanced voter privacy, and mobile-first DApp interfaces to improve accessibility for rural populations. Integration with Aadhaar-based biometric authentication is also planned to strengthen the identity verification layer.

REFERENCES

[1] B. Sujatha, Y. Ganesh, N. Leelavathy, R. Tamilkodi, S. Venkatesh, B. Sandhya and T. S. Kowshik, "Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication, Online Voting and Election Automation,"Indian Journal of Science and Technology, vol. 17, no. 47, pp. 4948-4958, 2024.
[2] A. Singh, "Secure Voting Website Using Ethereum and Smart Contracts," Future Internet, vol. 6, no. 4, 2023.
[3] U. Jafar, S. I. Ali, and M. Waqas, "Blockchain for Electronic Voting System Review and Open Research Challenges," IEEE Access, 2021.
[4] S. Alvi, A. Rehman, and M. A. Shah, "DVTChain: A Blockchain-Based Decentralized Mechanism to Ensure the Security of Digital Voting Systems," Journal of King Saud University - Computer and Information Sciences, 2022.
[5] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," Financial Cryptography and Data Security, 2017.
[6] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.
[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[8] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business and Information Systems Engineering, vol. 59, no. 3, pp. 183-187, 2017.
[9] K. Curran, E. Lunney, and J. Curran, "E-Voting on the Blockchain," Journal of Internet Technology and Secured Transactions, vol. 7, no. 1, 2018.
[10] N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," IEEE Software, vol. 35, no. 4, pp. 95-99, Jul./Aug. 2018.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY