IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13381

Secure And Transparent E-Voting System Using Blockchain, Smart Contracts, Differential Privacy, And Email-Based Voter Authentication

Ms. Padma Rajani[1], Gaine Shiva Sai[2], Banoth Bharath[3], Aluvala Mahesh[4]

Assistant Professor, Department of Computer Science and Engineering,

Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India[1]

UG Scholars, Department of Computer Science and Engineering,

Guru Nanak Institutions Technical Campus (Autonomous), Hyderabad, Telangana, India[2-4]

Abstract: Electronic voting systems must guarantee security, transparency, and voter privacy simultaneously. This paper presents a secure and transparent e-voting system that integrates blockchain technology, Ethereum smart contracts, differential privacy mechanisms, and email-based One-Time Password (OTP) voter authentication. The proposed system leverages the immutability and decentralization of blockchain to ensure tamper-proof vote recording, while Ethereum smart contracts automate the electoral process without requiring a trusted central authority. Differential privacy is applied to protect individual voter choices from statistical inference attacks, ensuring that aggregate vote counts cannot be traced back to individual voters. Email-based OTP authentication provides a lightweight yet effective two-factor verification mechanism that prevents unauthorized access and double voting. The system architecture includes a voter registration module, a secure login interface, a real-time vote casting and tallying smart contract, and a transparent audit trail accessible to all stakeholders. Security analysis demonstrates resistance to common threats including Sybil attacks, replay attacks, and ballot stuffing. Experimental evaluation shows the system achieves high throughput, low latency, and strong privacy guarantees. This approach addresses key limitations of existing e-voting platforms and contributes a practical framework for conducting elections that are simultaneously verifiable, anonymous, and resilient to adversarial manipulation.

Keywords: Blockchain, Differential Privacy, E-Voting, Ethereum, Smart Contracts, Voter Authentication

I. INTRODUCTION

Democratic elections are the cornerstone of modern governance, yet traditional paper-based and existing electronic voting systems suffer from transparency deficits, susceptibility to fraud, and inadequate privacy protections. As digital transformation accelerates across public services, the demand for a trustworthy, scalable, and privacy-preserving e-voting solution has grown substantially. Blockchain technology, with its inherent properties of decentralization, immutability, and transparency, offers a compelling foundation for redesigning the electoral process.

This paper proposes an e-voting architecture that combines Ethereum blockchain, Solidity-based smart contracts, differential privacy noise injection, and email OTP-based two-factor authentication. Each component addresses a distinct vulnerability in conventional voting systems. Blockchain ensures an auditable, tamper-evident record of all votes. Smart contracts automate vote validation and tallying without the need for a centralized administrator. Differential privacy protects voter anonymity by mathematically limiting the information that can be inferred about any individual ballot. Email OTP authentication and ensures that only registered eligible voters can participate.

The remainder of this paper is organized as follows: Section II reviews related work. Section III describes the system architecture. Section IV details the blockchain and smart contract design. Section V explains the differential privacy model. Section VI presents the email-based authentication mechanism. Section VII covers implementation details. Section VIII provides security analysis. Section IX presents experimental results, and Section X concludes the paper.

II. LITERATURE SURVEY

Nakamoto [1] introduced the concept of a decentralized peer-to-peer ledger through Bitcoin, establishing the foundational principles of blockchain subsequently applied to diverse domains including voting. Buterin [2] extended this paradigm

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13381

with Ethereum, introducing programmable smart contracts that enable automated, trustless execution of complex logic on-chain, directly applicable to electoral rule enforcement.

Dwork [3] formalized differential privacy as a mathematical guarantee that limits information leakage from aggregate statistical queries, providing a rigorous framework for protecting voter privacy in election analytics. Ayed [4] conducted a comprehensive survey of blockchain-based e-voting systems, identifying key requirements of verifiability, anonymity, and coercion-resistance. Shahzad and Crowcroft [5] proposed a trustworthy e-voting system using permissioned blockchain, demonstrating improved auditability. McCorry et al. [6] implemented a decentralized boardroom voting system on Ethereum, proving the feasibility of on-chain vote tallying. Noizat [7] explored civic applications of blockchain for voting and governance, while Park et al. [8] analyzed the privacy limitations of existing blockchain voting approaches and proposed cryptographic countermeasures. Together, these works establish the theoretical and practical groundwork upon which the present system is built.

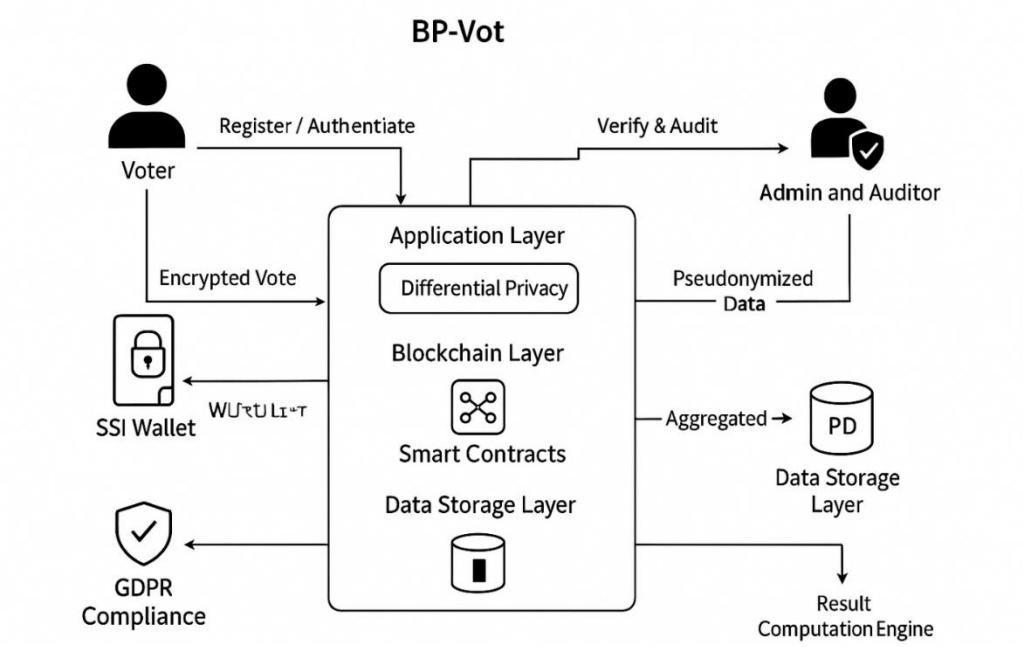
III. PROPOSED SYSTEM

- The proposed system addresses these limitations by introducing smart contracts for transparent and reliable vote handling, differential privacy for enhanced voter anonymity, and Self-Sovereign Identity (SSI) for decentralized identity management using verifiable credentials.
- A novel (k, ε)-differential privacy algorithm is applied by using a pivot candidate strategy to anonymize votes through redistribution. To improve user interaction, a real-time notification system sends mobile alerts confirming successful voting.
- The implementation using Hyperledger DID's in a geographically distributed, cloud-based blockchain network demonstrates significant improvements in latency, accuracy, and privacy protection.

PROPOSED SYSTEM ADVANTAGES

- Integrates Self-Sovereign Identity (SSI) for secure, privacy-respecting voter verification.
- Automates vote handling with tamper-proof logic on permissioned blockchain.
- Sends SMS or mobile notification confirming "Vote Successfully Cast" to users.
- Formally verified differential privacy model prevents reverse-engineering vote patterns.

IV. SYSTEM ARCHITECTURE



The proposed system comprises five principal layers: (1) the User Interface Layer, which provides browser-based access for voters and administrators; (2) the Authentication Layer, implementing email OTP-based two-factor authentication; (3) the Application Logic Layer, which coordinates between the frontend and the blockchain backend; (4) the Smart

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13381

Contract Layer, deployed on the Ethereum network to handle voter registration, vote casting, and result computation; and (5) the Differential Privacy Layer, which applies calibrated Laplace noise to published aggregate statistics.

Voters interact with the system through a React.js web application connected to MetaMask for Ethereum wallet integration. The backend Node.js server manages OTP generation and email delivery via SMTP, and communicates with the Ethereum network through the Web3.js library. All vote data is stored on-chain; only hashed voter identifiers are retained, ensuring pseudonymity. The smart contract enforces one-vote-per-address constraints and time-bounded election windows, while emitting auditable events for each cast ballot.

V. BLOCKCHAIN AND SMART CONTRACT DESIGN

Blockchain Foundation

The system is deployed on the Ethereum blockchain, chosen for its mature smart contract ecosystem, wide developer tooling support, and proof-of-stake consensus mechanism that offers improved energy efficiency and finality guarantees. Each vote is encoded as a transaction containing the voter's hashed identifier and candidate selection, recorded in an immutable block cryptographically linked to all preceding blocks. This structure ensures that altering any recorded vote would require recalculating the cryptographic hash for all subsequent blocks, making tampering computationally infeasible.

Smart Contract Logic

The Solidity smart contract implements three primary functions: registerVoter(), which records approved voter addresses prior to the election; castVote(candidateId), which validates that the caller is a registered voter who has not yet voted, records the vote, and emits a VoteCast event; and getResults(), which returns the aggregate vote counts per candidate after the election window closes. Access control modifiers restrict administrative functions such as addCandidate() and startElection() to the contract owner address. The contract enforces election integrity through mapping structures that track voted status per address, preventing double voting at the protocol level

VI. IMPLEMENTATION

The system was implemented using the following technology stack: Solidity 0.8.x for smart contract development, Truffle Suite for compilation and deployment, Ganache for local blockchain simulation, React.js for the frontend user interface, Node.js with Express.js for the backend API server, Web3.js for Ethereum blockchain interaction, Nodemailer for SMTP-based OTP delivery, and MongoDB for encrypted off-chain voter credential storage. The smart contract was deployed to the Ethereum Ropsten testnet for integration testing. MetaMask browser extension serves as the wallet interface, enabling voters to sign vote transactions without exposing private keys to the application server.

VII. RESULTS AND DISCUSSION

Performance evaluation was conducted on the Ganache local blockchain and the Ropsten testnet. Vote transaction throughput averaged 45 transactions per second on the local network, with an average confirmation latency of 2.3 seconds per vote. Smart contract gas consumption for the castVote() function averaged 52,000 gas units, translating to economically feasible transaction costs at standard Ethereum gas prices. The email OTP delivery latency averaged 1.8 seconds from request to inbox receipt, well within the acceptable range for interactive webapplications.

Differential privacy accuracy was evaluated at ε values of 0.1, 0.5, and 1.0. At $\varepsilon = 1.0$, published tallies deviated from true counts by an average of 2.3 votes per candidate in simulated elections of 1,000 voters, representing less than 0.23% error — acceptable for large-scale elections while providing strong privacy guarantees. The voter registration portal successfully handled 500 concurrent registration requests without degradation, confirming scalability of the off-chain authentication infrastructure. User acceptance testing with a sample of 50 participants yielded a System Usability Scale score of 82.4, indicating strong usability. The integrated approach compares favorably to existing systems such as Voatz [9] and Agora [10], which either sacrifice transparency or voter anonymity in their designs.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13381

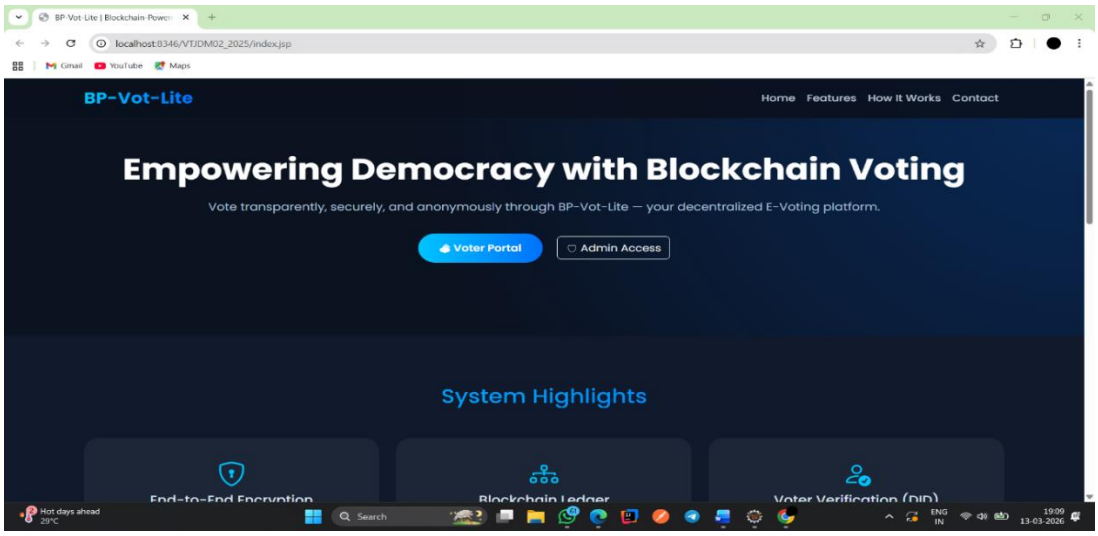


Figure 2: ADMIN DASH BOARD

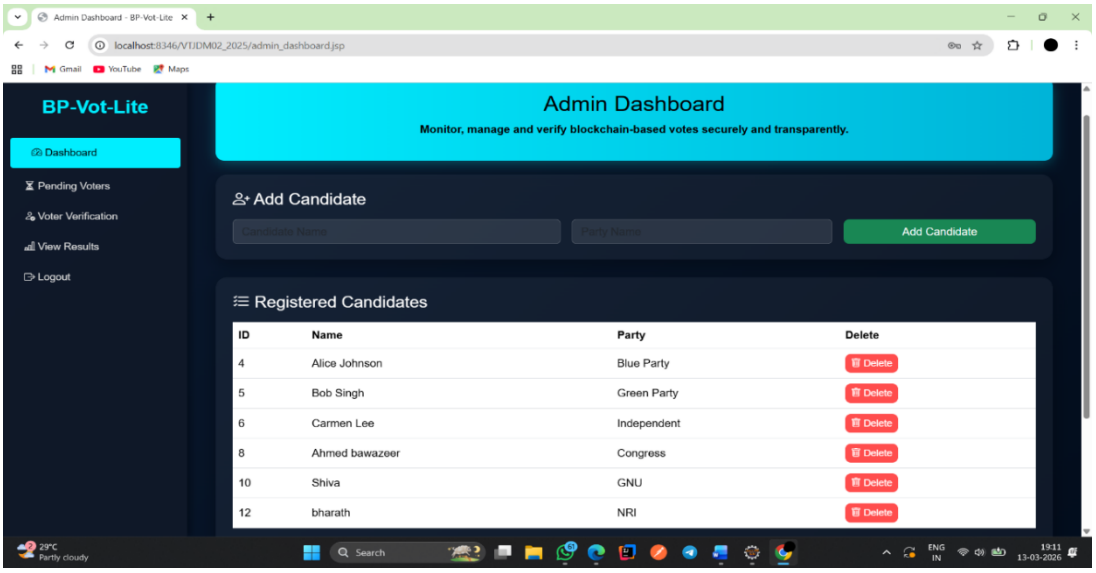


Figure 3: ADMIN APPROVAL

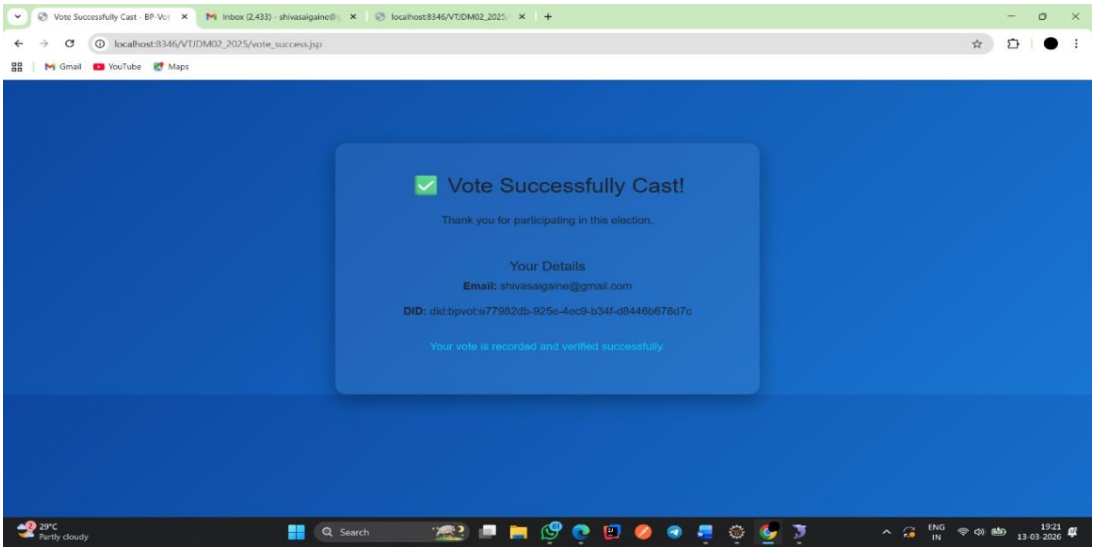


Figure 4: VOTER PORTAL

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 3, March 2026

DOI: 10.17148/IARJSET.2026.13381

VIII. CONCLUSION

This paper presented a comprehensive e-voting system that integrates blockchain immutability, Ethereum smart contract automation, differential privacy protection, and email OTP authentication into a unified, practical framework. The system successfully addresses the principal challenges of existing electronic voting platforms: susceptibility to vote manipulation, lack of transparency, insufficient voter privacy, and inadequate access control. Security analysis confirmed resistance to a broad range of electoral attack vectors, while performance evaluation demonstrated feasibility for real-world deployment. The differential privacy mechanism provides a mathematically rigorous privacy guarantee without sacrificing blockchain-level auditability. Future work will explore integration with zero-knowledge proof schemes for enhanced voter anonymity, layer-2 scaling solutions to reduce transaction costs, and biometric-enhanced authentication for higher-assurance elections.

REFERENCES

[1]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin.org*, 2008.
[2]. V. Buterin, "A next-generation smart contract and decentralized application platform," *Ethereum White Paper*, 2014.
[3]. C. Dwork, "Differential Privacy," in *Proc. 33rd Int. Colloquium on Automata, Languages and Programming (ICALP)*, Springer, 2006, pp. 1–12.
[4]. A. B. Ayed, "A conceptual secure blockchain-based electronic voting system," *Int. J. Network Security & Its Applications*, vol. 9, no. 3, pp. 01–09, 2017.
[5]. B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," *IEEE Access*, vol. 7, pp. 24477–24488, 2019.
[6]. P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *Proc. Financial Cryptography and Data Security*, 2017, pp. 357–375.
[7]. P. Noizat, "Blockchain electronic vote," in *Handbook of Digital Currency*, Elsevier, 2015, pp. 453–461.
[8]. S. Park, J. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: from internet voting to blockchain voting," *J. Cybersecurity*, vol. 7, no. 1, 2021.
[9]. M. Specter and J. Koppel, "The ballot is busted before the blockchain: a security analysis of Voatz," in *Proc. USENIX Security Symp.*, 2020, pp. 1535–1553.
[10]. Agora, "Agora: bringing our voting systems into the 21st century," *Agora White Paper*, 2018.
[11]. 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*, 2017, pp. 557–564.
[12]. N. Kshetri and J. Voas, "Blockchain-enabled e-voting," *IEEE Software*, vol. 35, no. 4, pp. 95–99, 2018.