ISSN 2277-2685
IJESR/April. 2026/ Vol-16/Issue-2s1/202-206
Mohammed Museb Ahmed *et. al.,* / International Journal of Engineering & Science Research

Full Length Article

Secure And Transparent E-Voting System Using Blockchain, Smart Contracts, Differential Privacy, And Self-Sovereign Identity

Mohammed Museb Ahmed[1], Mohammed Abdullah Shareef[2], Md Abubakar Siddique[3], Mr. Syed Zaffar Mahmood[4]
[1,2,3]B.E.Students ;Department of Information Technology ISL Engineering College Osmania University Hyderabad India.
[4]Associate Professor; Department of Information Technology ISL Engineering College Osmania University Hyderabad India.
Mail Id; mohammadmusebahmed@gmail.com , Shareefabd659@gmail.com, 160522737065@islec.edu.in
Accepted 25-04-2026

Abstract
Electronic voting systems have become increasingly significant in modern democratic environments due to the growing demand for transparency, scalability, and digital accessibility. Traditional voting systems suffer from challenges such as centralized control, vote tampering, lack of transparency, operational delays, and high management costs. Although blockchain technology has emerged as a revolutionary solution for secure digital transactions, many existing blockchain-based voting systems still fail to achieve strong voter privacy, efficient scalability, and regulatory compliance. This paper presents BP-Vot-Lite, a secure and transparent blockchain-enabled electronic voting framework integrating smart contracts, differential privacy, and Self-Sovereign Identity (SSI). The framework ensures voter anonymity, immutable vote storage, transparent result verification, and decentralized identity management. Differential privacy mechanisms are employed to prevent reconstruction attacks while maintaining statistical accuracy in election outcomes. Experimental analysis demonstrates improved latency, enhanced privacy preservation, and reliable performance in distributed blockchain environments. The proposed architecture contributes toward developing secure, transparent, scalable, and privacy-preserving digital election systems suitable for modern e-governance applications.

Keywords
Blockchain, Electronic Voting, Smart Contracts, Differential Privacy, Self-Sovereign Identity, Hyperledger Besu, Privacy Preservation, Secure Voting, Decentralized Systems.

Introduction

Voting plays a fundamental role in preserving democratic values and ensuring fair representation in society. Conventional voting systems are generally paper-based and rely heavily on centralized authorities for election management and vote counting. Such systems often suffer from issues including vote manipulation, long processing times, human errors, and lack of transparency. With the advancement of digital technologies, electronic voting systems have emerged as an alternative approach for improving election efficiency and accessibility. However, many electronic voting systems remain vulnerable to cyberattacks, centralized failures, and privacy breaches. Blockchain technology introduces decentralization, immutability, transparency, and distributed consensus, making it a promising solution for next-generation voting systems. Blockchain-based voting systems store votes as immutable transactions, ensuring transparency and tamper resistance. Despite these advantages, blockchain voting systems face several challenges including scalability limitations, privacy concerns, and voter identity management. Public blockchain ledgers expose transaction visibility, which may compromise voter anonymity. Therefore, integrating privacy-preserving mechanisms becomes essential for secure electronic voting. The proposed BP-Vot-Lite framework combines blockchain technology with differential privacy and Self-Sovereign Identity to create a secure, decentralized, and transparent voting ecosystem. The framework uses smart contracts to automate vote validation and result computation while preserving voter anonymity through advanced cryptographic and privacy-preserving methods.

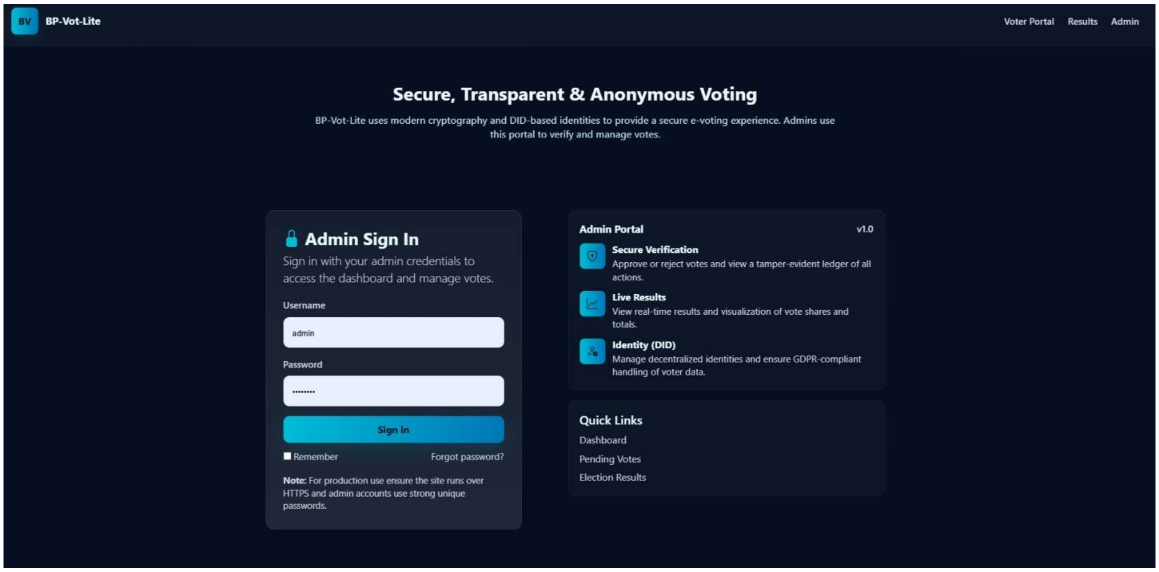

Figure 1: BP-Vot-Lite System Homepage and Feature Highlights

Problem Statement

Traditional voting systems rely on centralized infrastructures that are prone to tampering, corruption, operational inefficiencies, and lack of transparency. Existing electronic voting systems often suffer from vulnerabilities related to authentication, vote integrity, and data breaches. Although blockchain technology improves transparency and immutability, the public nature of distributed ledgers introduces privacy risks that may expose voter behavior. Many existing blockchain-based voting systems also fail to achieve scalability under large transaction loads and do not adequately address regulatory compliance requirements such as GDPR. Additionally, centralized identity verification mechanisms increase the risks of identity theft and unauthorized access. Therefore, there is a need for a decentralized and privacy-preserving voting framework that ensures transparency, anonymity, scalability, and secure voter authentication simultaneously.

Objectives

- To design a decentralized blockchain-based electronic voting framework.
- To preserve voter anonymity using differential privacy mechanisms.
- To implement smart contracts for secure vote validation and automation.
- To integrate Self-Sovereign Identity for decentralized authentication.
- To ensure transparency and tamper-proof vote storage.
- To provide scalable and efficient transaction processing.
- To maintain compliance with privacy regulations such as GDPR.
- To improve user trust and election auditability through immutable blockchain records.

Literature Survey

Several researchers have proposed blockchain-enabled electronic voting frameworks to improve election security and transparency. Tanwar et al. developed an Ethereum-based decentralized voting application using smart contracts to ensure transparency and secure vote recording. Their work highlighted the potential of blockchain in minimizing election fraud and improving public trust. Xue et al. proposed ACB-Vote, a blockchain-based score voting system utilizing anonymously convertible ballots and privacy-preserving signatures. Their approach improved anonymity and flexible vote tallying while maintaining blockchain integrity. Mukherjee et al. introduced a blockchain-based e-voting framework emphasizing voter anonymity and tamper-proof vote recording. The system focused on preventing illegitimate voting and ensuring election fairness through Ethereum smart contracts. Sallal et al. proposed the PVPBC framework, which combined privacy and verifiability using permissioned blockchain architecture and revocable anonymity techniques. Their work demonstrated scalability and low authorization latency. Although previous studies improved election transparency and decentralization, many failed to simultaneously address privacy, scalability, usability, and regulatory compliance. The BP-Vot-Lite framework extends prior research by integrating differential privacy, decentralized SSI authentication, and optimized blockchain deployment within a unified secure voting architecture.

Proposed System and Methodology

The BP-Vot-Lite framework integrates blockchain, differential privacy, smart contracts, and Self-Sovereign Identity to establish a secure electronic voting environment. The architecture consists of multiple layers including voter registration, authentication, vote casting, blockchain storage, result aggregation, and visualization modules. During registration, voters generate decentralized digital identities using SSI mechanisms. Public and private cryptographic keys are securely generated and stored within decentralized identity wallets. The administrator verifies voter credentials before granting election participation rights. When a voter casts a vote, the vote is encrypted using asymmetric cryptography and transmitted as a blockchain transaction. Smart contracts validate transaction integrity and ensure one-vote-per-user policies. The blockchain ledger records all verified transactions immutably, enabling transparent auditing and tamper resistance. To preserve privacy, differential privacy mechanisms introduce carefully calibrated noise during vote aggregation. This prevents adversaries from identifying individual voting behavior while maintaining accurate statistical outcomes. The proposed framework also supports notification services that inform voters once votes are securely recorded.

Figure 2: Voter Registration Module

Figure 3: Pending Voter Registrations – Admin Verification Panel

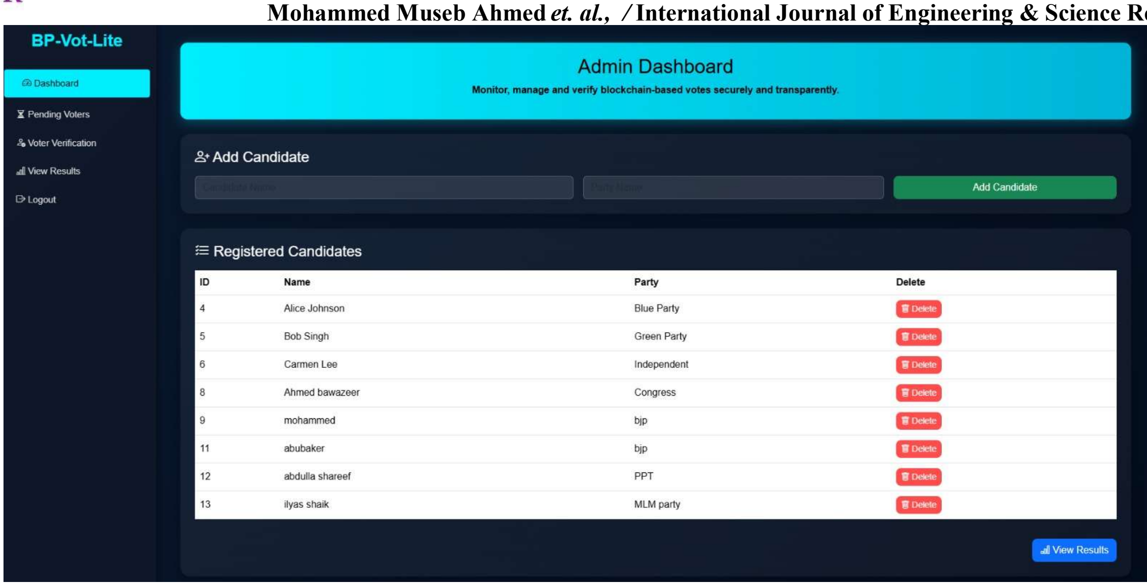

Figure 4: Admin Authentication Module – Secure Sign-In Portal

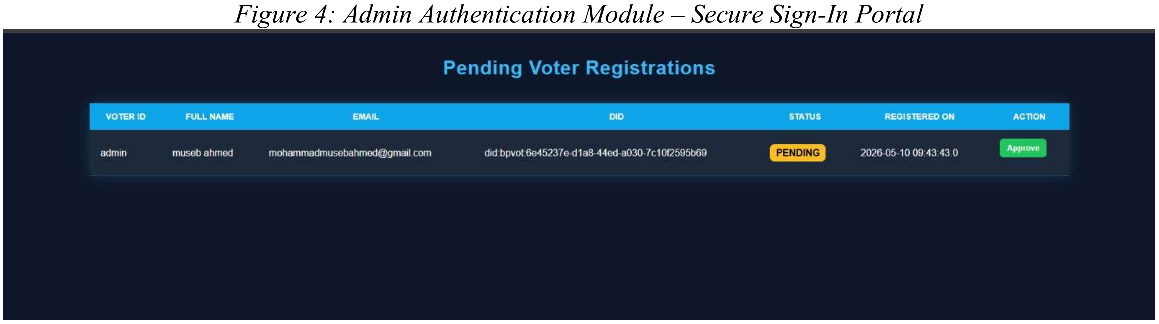

Figure 5: Admin Dashboard – Candidate Management and Voting Results

System Modules

The BP-Vot-Lite system consists of several interconnected modules:

User Authentication Module:
Provides secure login and role-based access control for voters and administrators using encrypted credentials and session validation.
Voter Registration Module:
Allows users to securely register by submitting personal information and digital credentials. The module validates uniqueness and stores encrypted records.
VoterVerificationModule:
Enables administrators to verify voter authenticity and approve legitimate registrations.
CandidateManagementModule:
Allows administrators to add, modify, and manage candidate details for elections.
Voting Module:
Facilitates secure vote casting through blockchain-integrated encrypted transactions.
Vote Validation Module:
Validates blockchain transactions and ensures integrity of recorded votes.
Result Visualization Module:
Displays election outcomes through graphs, charts, and real-time statistical summaries.
Blockchain Ledger Module:
Maintains immutable blockchain records for all verified voting activities and audit logs.

Technologies Used

• Java EE (JSP and Servlets) for frontend and backend integration.
• Hyperledger Besu for distributed blockchain infrastructure.
• MySQL Database for structured data management.
• Apache Tomcat Server for deployment.
• Differential Privacy algorithms for vote anonymization.
• Self-Sovereign Identity mechanisms for decentralized authentication.
• Eclipse IDE / IntelliJ IDEA for software development.
• SHA-256 and cryptographic encryption algorithms for secure vote storage.
• Chart.js and graphical tools for result visualization.

ISSN 2277-2685
IJESR/April. 2026/ Vol-16/Issue-2s1/202-206
Mohammed Museb Ahmed *et. al.*, / International Journal of Engineering & Science Research

Implementation Details

Results and Discussion

The BP-Vot-Lite framework was evaluated under distributed blockchain environments using geographically separated Hyperledger Besu nodes. Experimental observations indicated improved transaction throughput and lower latency compared to traditional blockchain-based voting systems.

The framework consistently maintained more than 98% result accuracy while applying differential privacy mechanisms. Vote transactions were securely validated and recorded on immutable blockchain ledgers. SSI-based authentication improved privacy by eliminating centralized identity dependencies.

The system successfully handled large voting loads without significant performance degradation, demonstrating scalability suitable for real-world democratic elections. Differential privacy effectively prevented reconstruction attacks while preserving election transparency and auditability.

Advantages

• Secure decentralized voting architecture.
• Tamper-proof blockchain-based vote storage.
• Enhanced voter anonymity using differential privacy.
• Transparent and auditable election process.
• Secure decentralized identity management through SSI.
• Smart contract automation reduces manual intervention.
• Improved scalability and transaction efficiency.
• GDPR-compliant privacy-preserving framework.
• Real-time result visualization and notification services.

Future Scope

Future enhancements can further strengthen the BP-Vot-Lite framework by integrating biometric authentication, artificial intelligence-based fraud detection, and mobile voting support. Advanced cryptographic approaches such as zero-knowledge proofs and post-quantum encryption algorithms may also improve long-term security. Cloud-native blockchain deployment and optimized consensus mechanisms can increase scalability for nationwide elections. Integration with national identity systems and multilingual user interfaces may further improve usability and adoption. Additionally, AI-driven analytics can enhance election monitoring and anomaly detection capabilities.

Conclusion

The BP-Vot-Lite framework presents a secure, transparent, scalable, and privacy-preserving electronic voting system integrating blockchain, differential privacy, smart contracts, and Self-Sovereign Identity. The framework successfully addresses major challenges in conventional and existing blockchain-based voting systems including privacy leakage, tampering risks, centralized identity dependence, and scalability limitations. Experimental analysis demonstrated improved transaction efficiency, reliable vote integrity, and strong privacy guarantees under distributed blockchain environments. The proposed framework contributes toward developing trustworthy digital democratic systems capable of supporting secure and transparent elections in modern e-governance environments.

References

[1] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, “Implementation of blockchain-based e-voting system,” 2024.
[2] W. Xue, Y. Yang, Y. Li, H. Pang, and R. H. Deng, “ACB-Vote: Efficient, flexible, and privacy-preserving blockchain-based score voting,” 2023.
[3] A. Mukherjee, S. Majumdar, A. Kumar Kolya, and S. Nandi, “A privacy preserving blockchain-based E-voting system,” 2023.
[4] M. Sallal, R. de Fréin, and A. Malik, “PVPBC: Privacy and verifiability preserving E-voting based on permissioned blockchain,” 2023.
[5] A. Alshehri, M. Baza, G. Srivastava, and others, “Privacy-preserving E-voting system supporting score voting using blockchain,” 2023.
[6] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[7] Hyperledger Foundation Documentation, “Hyperledger Besu,” 2024.
[8] GDPR Official Documentation, European Union Data Protection Regulation, 2023.