As per UGC guidelines an electronic bar code is provided to secure your paper

International Journal for Modern Trends in Science and Technology
Volume 12, Issue 04, pages 1177-1178
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue04.html
DOI: https://doi.org/10.5281/zenodo.19668244

Blockchain-Based Secure Voting System

S . Usha Baby, K. Tanmayee, K. Sumathi, T. Yasaswini, K. Sharonu

Department of CSE, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada.

To Cite this Article
S . Usha Baby, K. Tanmayee, K. Sumathi, T. Yasaswini & K. Sharonu (2026). Blockchain-Based Secure Voting System. International Journal for Modern Trends in Science and Technology, 12(04), 1177-1178. https://doi.org/10.5281/zenodo.19668244

Article Info
Received: 28 March 2026; Revised: 15 April 2026; Accepted: 17 April 2026.

KEYWORDS

ABSTRACT

Secure Vote is a decentralized, transparent, and tamper-proof electronic voting system built using Blockchain technology and Django framework. The system ensures vote integrity by cryptographically sealing each vote as a block in an immutable ledger. It eliminates centralized manipulation, ensures voter anonymity through SHA-256 hashing, and provides real-time verification via a Block Explorer dashboard.

1. INTRODUCTION

1.1. Objectives:

- To develop a secure web-based e-voting platform using Django.
- To implement a custom Blockchain ensuring immutability of votes.
- To provide transparency through a public Block Explorer.
- To prevent double voting using hybrid SQL + Blockchain validation.
- To ensure cryptographic anonymity of voters.

2. METHODOLOGY:

The system follows a hybrid Web-Blockchain architecture. Votes are captured through Django views, validated against relational database constraints, then anonymized using SHA- 256 hashing. Each vote is converted into a block containing index, timestamp, vote data, previous hash, and nonce. Blocks are cryptographically linked to form an immutable chain.

3. SYSTEM DESIGN:

The system uses a layered architecture:

1. User Interface Layer – HTML, CSS, JavaScript.
2. Backend Logic Layer – Django framework (MVT architecture).
3. Blockchain Core Module – Custom Python Blockchain engine.
4. Database Layer – SQLite/PostgreSQL for relational data.
5. Security Layer – SHA-256 hashing, CSRF protection, role-based access

4.KEY FEATURES:

- Blockchain-backed vote integrity.
- Real-time Block Explorer for transparency.

• Role-Based Access Control (Admin, Voter, Candidate).
• Double-voting prevention mechanism.
• Tamper-evident ledger validation system.

5.RESULTS:

The prototype successfully records votes as blockchain transactions. Testing confirmed 100% detection of tampering attempts and accurate prevention of duplicate voting. Vote confirmation time averaged under 1 second with moderate hashing difficulty.

6.CONCLUSION

Secure Vote demonstrates that Blockchain technology can enhance electoral transparency, integrity, and trust. The hybrid architecture combines the speed of relational databases with the immutability of blockchain ledgers, making it a viable solution for institutional and governmental elections.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
[2] Django Documentation 4.2.
[3] NIST Secure Hash Standard (FIPS PUB 180-4).
[4] Baudier et al. (2019). Trust in Blockchain Voting Systems.