WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Secure Hybrid Blockchain-Based E-Voting System with Biometric Authentication and Fraud Detection

Guide: Dr. Neelambike S[1], A S Pranam[2], Chetan S S[2], Nachiketh L B[2], Vishwanath H[2]

[1] Guide – Professor & Head of the Department, Department of Information Science and Engineering
[2] Student Scholars, Department of Information Science and Engineering
[1,2] GM Institute of Technology, Davanagere
Email : pranamas98@gmail.com, chetanshirageri@gmail.com, nachiketh1710@gmail.com, vishwanathhbn@gmail.com

A B S T R A C T :

Online voting can make elections easier to administer and more accessible to voters who cannot conveniently reach a polling station. However, a remote voting system must establish voter identity, prevent repeated voting, preserve recorded vote integrity, and identify suspicious activity. This paper presents Ledger Vote, a hybrid electronic voting system that combines face authentication, liveness detection, duplicate-face prevention, rule-based fraud scoring, and a custom SHA-256 hash-chain ledger.

The system uses MediaPipe for face detection and blink and head-turn liveness checks, while InsightFace generates 512-dimensional ArcFace embeddings. Facial embeddings are encrypted using AES before storage. Routine user and election information is maintained in PostgreSQL, while each accepted vote is stored as a block in a custom Python-based SHA-256 hash chain. Functional and adversarial testing examined duplicate identities, repeated voting, suspicious activity, role restrictions, concurrent submissions, and ledger tampering.

Keywords: Electronic Voting, Blockchain, Hash Chain, Biometric Authentication, Face Recognition, Liveness Detection, Fraud Detection, Tamper Detection, Role-Based Access Control.

1. Introduction

Public confidence matters to an election as much as the final count. Paper ballots are familiar, but they can require considerable time and administrative effort, particularly when voters are remote or have limited mobility. Electronic and Internet voting can reduce some of these difficulties, but moving the process online introduces security concerns such as voter impersonation, repeated voting, and unauthorized changes to stored election information.

A dependable remote voting platform must restrict voting to eligible participants, ensure that each voter casts no more than one ballot in an election, preserve the integrity of recorded votes, and provide audit information for administrators. Existing approaches often address only part of this problem. Public blockchain systems can introduce transaction costs and confirmation delays, while biometric authentication alone does not prove that stored election records remain unchanged.

Ledger Vote addresses these requirements through a hybrid design. PostgreSQL stores users, elections, eligibility, and administrative information, while accepted votes are recorded in a custom SHA-256 hash chain implemented in Python. The platform combines face verification, liveness checks, fraud scoring, role-based access control, and ledger verification within one institutional voting workflow.

For vote recording, each accepted vote is stored as a new block containing information such as the block index, timestamp, transaction identifier, vote data, previous block hash, and current block hash. The system uses database row locking during block creation to maintain consistency when multiple voting requests occur simultaneously. An authorized administrator can use the Blockchain Explorer to inspect stored blocks and verify the chain by recalculating hashes and checking the links between consecutive blocks.

The proposed Ledger Vote system integrates biometric authentication, liveness detection, duplicate-identity prevention, fraud scoring, role-based access control, and hash-chain-based vote storage within a single web-based application. It also provides administrative facilities for election management, fraud monitoring, audit-log inspection, result generation, and PDF and Excel report exports. The prototype is evaluated through functional and adversarial testing to examine its behaviour under different voting and security scenarios.

The main objective of this project is to develop a secure and manageable electronic voting platform that improves voter verification, helps prevent duplicate voting, and provides tamper-evident storage of accepted votes. The system demonstrates how multiple complementary security mechanisms can be integrated into an institutional voting environment while also identifying limitations that require further research and improvement.

2. Related Work

Research on electronic voting has examined voter authentication, ballot integrity, privacy, auditability, and resistance to repeated voting. Blockchain-based approaches use linked or distributed records to make unauthorized changes more difficult to conceal. However, public blockchain deployments may introduce transaction fees, confirmation delays, and operational dependencies.

2.1. Blockchain-Based Electronic Voting

Blockchain-based voting systems use cryptographic links or distributed consensus to protect recorded ballots and support verification. Prior work has explored scalable blockchain-shard architectures, privacy-preserving election systems, and hybrid voting frameworks [1], [2], [6], [11]. Ledger Vote adopts a custom SHA-256 hash chain rather than a public blockchain platform. This design avoids public-network transaction fees, but the ledger remains controlled by the application operator and is therefore tamper-evident rather than a distributed consensus network.

2.2. Biometric Authentication and Liveness Detection

Biometric authentication can strengthen the connection between a voter account and the person using it. Research has examined multimodal biometric verification and face-based voting systems [3], [5], [14]. Face embeddings support similarity comparison, while liveness checks help reduce the risk of accepting photographs or replayed images. Ledger Vote combines MediaPipe face and landmark detection with blink and head-turn challenges and InsightFace ArcFace embeddings.

2.3. Fraud Detection and Election Security

Anomaly detection and behavioural signals can help identify suspicious activity in online systems. In an election environment, repeated voting attempts, multiple sessions or devices, repeated authentication failures, and incomplete liveness checks may indicate abuse. Ledger Vote uses a transparent rule-based fraud score to evaluate these signals before a vote is appended to the ledger.

2.4. Research Gap

Existing studies have separately explored blockchain-based record storage, biometric authentication, and anomaly detection. Integrating these mechanisms into one operational voting workflow introduces additional design challenges. Ledger Vote combines identity verification, liveness detection, duplicate-face prevention, fraud scoring, role-based access control, and a custom hash-chain ledger in a single institutional platform.

3. Literature Survey

Recent research shows increasing use of blockchain technology, biometric authentication, and privacy-preserving techniques for improving the security and reliability of electronic voting systems. Studies focus on protecting stored votes, verifying voter identities, preventing unauthorized voting, maintaining ballot privacy, and improving the scalability and auditability of election systems. These developments provide the research foundation for Ledger Vote, which combines biometric authentication, liveness detection, fraud detection, and a custom SHA-256 hash-chain ledger.

3.1. Blockchain-Based Electronic Voting Systems

Joni et al. [1] proposed HAC-Bchain, a secure and scalable blockchain-shard-based electronic voting system. Their work focuses on improving the scalability and security of blockchain-based voting. Repe [2] presented a smart and scalable election system using blockchain technology, with particular attention to privacy preservation and anomaly detection. Ajao et al. [3] explored the integration of blockchain with multimodal biometric authentication to support secure and verifiable electronic voting.
Ledger Vote follows a similar direction by using a hash-chain-based ledger to maintain vote integrity. In addition, it combines face authentication and fraud monitoring within the voting process.

3.2. Privacy and Security in Blockchain-Based Voting

Poudel [4] proposed a quantum-secure and blockchain-integrated e-voting framework with identity validation. Borhan et al. [5] investigated a blockchain-enabled voting scheme that combines deep hybrid learning with biometric authentication. These studies highlight the importance of integrating identity verification and cryptographic techniques to improve electronic voting security.
Ledger Vote also combines biometric identity verification with cryptographic protection. It uses AES encryption to protect stored facial embeddings and SHA-256 hashing to link accepted votes in the ledger.

3.3. Blockchain Consensus and Privacy-Preserving Techniques

Barke and Srivastava [6] proposed ReVo, a hybrid consensus protocol for blockchain in the Internet of Things that uses reputation and voting mechanisms. Rawat [7] presented a blockchain-based voting system using zero-knowledge proofs to improve privacy and verifiability. Ma [8] proposed a blockchain-based e-voting approach that combines dual-authority certification with homomorphic encryption.
These studies demonstrate different approaches to improving trust, privacy, and verification in electronic voting. Ledger Vote uses a custom SHA-256 hash-chain mechanism to provide tamper evidence for recorded votes, while maintaining election and user information in a relational PostgreSQL database.

3.4. Smart Contracts and Secure E-Voting Frameworks

Baniata [9] proposed BP-Vot, a blockchain-based electronic voting system that integrates smart contracts, differential privacy, and self-sovereign identities. Zhang [10] presented an improved secure and efficient e-voting scheme based on blockchain systems. These approaches emphasize the importance of secure vote recording, privacy protection, and efficient electronic election processes.
Ledger Vote follows the broader objective of improving electronic voting security by integrating face recognition, liveness verification, duplicate-face detection, rule-based fraud scoring, and blockchain-based vote integrity within a single institutional voting platform.

4. Research Methodology

The proposed system follows a sequence of election setup, voter registration, biometric verification, fraud assessment, secure vote recording, and audit. The main phases are:

- **Election Setup and Voter Registration:** The Super Admin creates elections and assigns Election Admins. Eligible voters register and complete face enrollment.
- **Face Enrollment and Duplicate Detection:** MediaPipe detects a single face, and InsightFace generates a 512-dimensional ArcFace embedding. New embeddings are compared with existing voter templates to reject duplicate identities.
- **Liveness Detection and Face Verification:** The voter completes blink and head-turn challenges. The live embedding is compared with the enrolled template.
- **Fraud Risk Assessment:** The fraud component evaluates duplicate vote attempts, multiple sessions or devices, repeated failed logins, and liveness failures.
- **Blockchain Vote Recording:** An accepted vote is appended as a new block linked to the previous block through a SHA-256 hash.
- **Auditing and Result Generation:** Authorized administrators verify the chain, inspect audit and fraud records, and export election results.

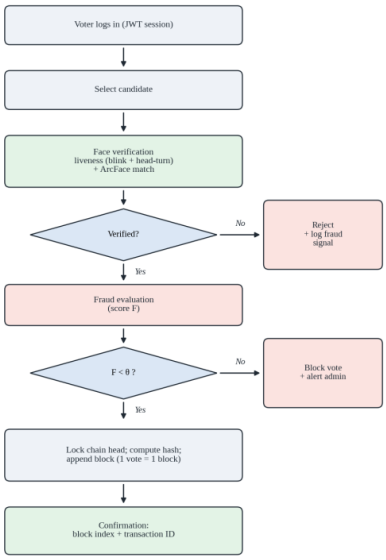


Fig. 1 – Workflow of the proposed voting and verification process

5. Implementation

Ledger Vote is implemented as a full-stack web application with a React-based front end, Flask back end, biometric processing components, and a PostgreSQL database hosted through Neon. Docker Compose is used to support deployment of the application components.

- **Frontend:** React 19 with Vite and Tailwind CSS provides the voter portal, election administration dashboard, blockchain explorer, and results and reports interface.
- **Backend:** Flask exposes REST APIs. SQLAlchemy manages database access, Alembic handles schema migrations, Marshmallow supports validation, and Flask-JWT-Extended provides token-based authentication.
- **Authentication and Roles:** Passwords are protected using bcrypt and JWT-based sessions. The system defines Super Admin, Election Admin, and Voter roles, with server-side permission checks.
- **Biometric Service:** MediaPipe performs face detection and blink and head-turn liveness checks. InsightFace generates ArcFace embeddings, which are encrypted using AES before storage.
- **Fraud and Ledger Service:** The fraud service evaluates risk indicators before vote acceptance. The ledger service locks the latest block, creates a new block, computes its SHA-256 hash, and stores the linked record.
- **Database and Audit:** PostgreSQL stores users, face templates, elections, candidates, eligibility, fraud events, audit logs, and ledger blocks. Administrative actions are recorded for review.
- **Election Management:** The Election Management module supports the election stages Draft, Scheduled, Live, Paused, and Closed. At least two candidates are required before an election becomes active, and candidate details are locked once voting begins.
- **Blockchain Verification:** Each accepted vote is stored as an individual block linked to the previous block. The verification mechanism recalculates block hashes and checks previous-hash relationships to identify modifications or inconsistencies in the ledger.
- **Admin Dashboard and Reports:** The dashboard allows authorized administrators to manage elections, monitor fraud events, inspect audit logs, and view election results. The system also supports exporting election information and reports in PDF and Excel formats.
- **Deployment:** Docker Compose is used to deploy the application components in separate containers, while Neon provides the managed PostgreSQL database for storing application and election information.

6. Results

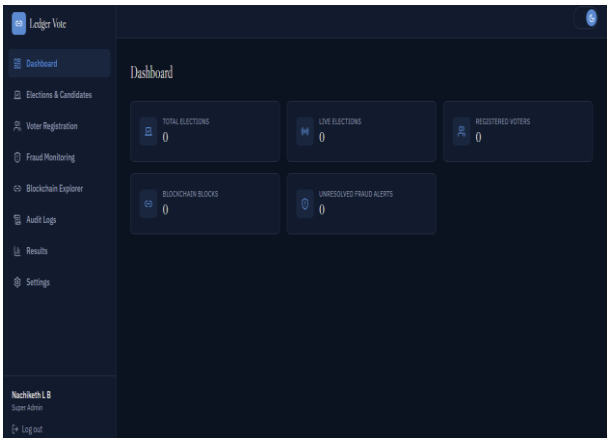


Fig. 2 –Admin Dashboard

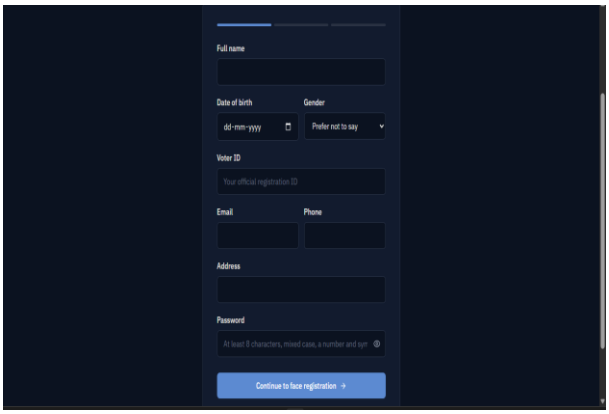


Fig. 3 –Voter Registration

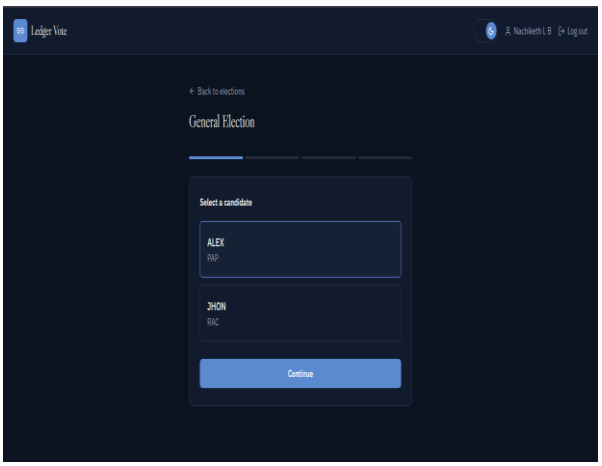


Fig. 4 –Candidate Selection

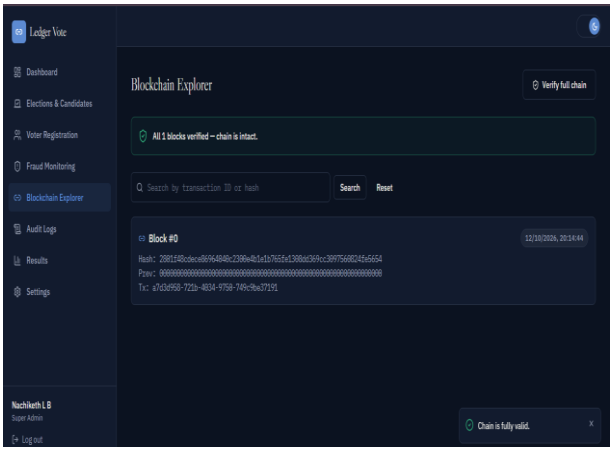


Fig. 5 –Blockchain Explorer

7. Conclusion

Ledger Vote presents a hybrid electronic voting prototype that integrates face authentication, liveness detection, duplicate-face prevention, rule-based fraud scoring, role-based access control, and a custom SHA-256 hash-chain ledger. Routine application information is maintained in PostgreSQL, while accepted votes are recorded as hash-linked blocks. Database row locking is used during block creation to maintain consistency when voting requests occur concurrently.

Functional and adversarial testing demonstrated that the implemented controls rejected duplicate identities and repeated voting attempts, flagged suspicious activity, detected the tested ledger modifications, enforced election-scoped access restrictions, and maintained a consistent chain during concurrent submissions. The prototype remains a research implementation. Its ledger is controlled by a single operator, liveness checks do not address every presentation attack, and it does not provide coercion resistance or complete end-to-end verifiability. Independent security assessment and larger-scale evaluation are required before use in higher-assurance elections.

ACKNOWLEDGEMENTS

The authors express their sincere gratitude to the Department of Information Science and Engineering, GM Institute of Technology, Davanagere, for providing the facilities, technical guidance, and academic support required to complete this work. The authors also thank their project guide and faculty members for their valuable suggestions, encouragement, and continuous support throughout the development of the project.

REFERENCES :

1. S. A. Joni, “HAC-Bchain: A Secure and Scalable Blockchain-Shard Based E-Voting System,” 2023 IEEE TEMSCON-ASPAC, Bengaluru, India, pp. 1–6, 2023, doi: 10.1109/TEMSCON-ASPAC59527.2023.10531344.
2. M. Repe, “Smart Secure and Scalable Election System using Blockchain with Privacy Preservation and Anomaly Detection,” 2025 IEEE GITCON, Belagavi, India, pp. 1–5, 2025, doi: 10.1109/GITCON65266.2025.11376972.
3. L. A. Ajao, “Blockchain Integration With Multimodal Biometric Authentication System for Secure Smart Verifiable Electronic Voting System,” IEEE Access, vol. 13, pp. 189850–189868, 2025, doi: 10.1109/ACCESS.2025.361897.
4. A. Poudel, “A Quantum-Secure and Blockchain-Integrated E-Voting Framework with Identity Validation,” 2025 IEEE CINS, Dubai, UAE, pp. 1–6, 2025, doi: 10.1109/CINS67018.2025.11412049.
5. R. Borhan, K. M. Mohi Uddin and M. Shorif Uddin, “Development of an E-Voting Scheme through a Blockchain-Enabled Approach with Deep Hybrid Learning for Biometric Authentication,” 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, pp. 1–6, 2024, doi: 10.1109/I2CT61223.2024.10543350.
6. S. Barke and G. Srivastava, “ReVo: A Hybrid Consensus Protocol for Blockchain in the Internet of Things through Reputation and Voting Mechanisms,” 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, pp. 1–8, 2024, doi: 10.1109/CCNC51664.2024.10454776.
7. S. S. Rawat, “A Blockchain-Based Voting System Using Zero-Knowledge Proofs for Enhanced Privacy and Verifiability,” 2025 International Conference on Computing, Intelligence, and Application (CIACON), Durgapur, India, pp. 1–6, 2025, doi: 10.1109/CIACON65473.2025.11189735.
8. L. Ma, “Blockchain-Based E-Voting with Dual-Authority Certification and Homomorphic Encryption,” 2026 5th International Informatics and Software Engineering Conference (IISEC), Ankara, Türkiye, pp. 40–45, 2026, doi: 10.1109/IISEC69317.2026.11418508.
9. H. Baniata, “BP-Vot: Blockchain-Based e-Voting Using Smart Contracts, Differential Privacy, and Self-Sovereign Identities,” IEEE Access, vol. 13, pp. 46106–46123, 2025, doi: 10.1109/ACCESS.2025.3548404.
10. J. Zhang, “An Improved Secure and Efficient E-Voting Scheme Based on Blockchain Systems,” IEEE Internet of Things Journal, vol. 12, no. 7, pp. 8626–8637, Apr. 2025, doi: 10.1109/JIOT.2024.3507366.