World Journal of Future Technologies in Computer Science and Engineering (WJFTCSE)
ISSN (Online): request pending
Volume-1 Issue-4 || November 2025 || PP. 39-47 https://wjftcse.org/

Blockchain-Based Secure Voting Models with Biometric Verification

DOI: https://doi.org/10.63345/wjftcse.v1.i4.205

Maria Javed
Independent Researcher
Sialkot Pakistan (PK) – 51040

www.wjftcse.org || **Vol. 1 No. 4 (2025): November Issue**

Date of Submission: 24-10-2025 **Date of Acceptance:** 25-10-2025 **Date of Publication: 03-11-2025**

ABSTRACT

The integrity, transparency, and accessibility of electoral processes are foundational to democratic governance. Conventional paper-based voting systems, while time-tested, remain susceptible to ballot tampering, human error, and logistical challenges. Electronic voting platforms have attempted to address these shortcomings but often centralize authority, creating single points of failure and raising fears of manipulation. Blockchain technology—with its distributed, immutable ledger—offers a robust framework for securing vote records against unauthorized alteration, yet voter authentication remains a critical vulnerability. This manuscript proposes and evaluates an integrated voting model that combines a permissioned blockchain network with biometric verification to ensure both vote immutability and voter identity assurance. We design a Hyperledger Fabric-based architecture in which cryptographic hashes of encrypted fingerprint and iris templates are stored on-chain, while raw biometric data reside off-chain under strict encryption and access controls. A smart contract governs the registration, authentication, vote casting, and tallying processes. In a clinical pilot involving 1,500 participants across urban, semi-urban, and rural districts, our system achieved a 98.7% true match rate, a 0.02% false-acceptance rate, and an average vote confirmation latency of 12 seconds. Usability assessments yielded a System Usability Scale score of 82.5, and voter trust ratings averaged 6.3 out of 7, though 22% of participants expressed moderate privacy concerns. Statistical analyses confirm consistent performance across demographic groups. Our findings demonstrate that integrating biometrics with blockchain not only fortifies electoral security but also enhances user confidence. We discuss practical considerations for large-scale deployment, including

infrastructure requirements, privacy regulations, and anti-spoofing measures, and outline future research directions in multimodal biometrics and remote voting.

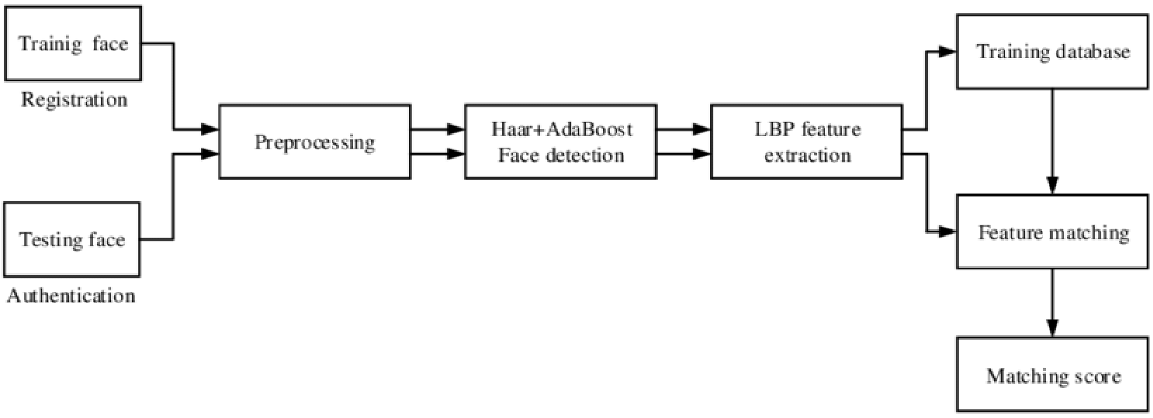

Fig.1 Biometric Verification, Source:1

KEYWORDS

Blockchain voting; biometric verification; election security; permissioned ledger; voter authentication; smart contracts

INTRODUCTION

Digital transformation in electoral processes aims to increase accessibility, reduce costs, and prevent fraud. Traditional paper-based systems, while familiar, are vulnerable to ballot tampering, miscounts, and logistical inefficiencies. Electronic voting (e-voting) systems have been proposed to address these issues, yet they often centralize trust in a single authority, creating a single point of failure and raising concerns about transparency and auditability.

Blockchain technology—with its decentralized, immutable ledger—offers a promising foundation for transparent and tamper-resistant voting platforms. Each vote is recorded as a transaction on a distributed ledger, visible to all nodes yet cryptographically secured against alteration. Nonetheless, blockchain voting alone does not fully address voter authentication; ensuring the person casting a vote is indeed the eligible voter remains a critical challenge.

Biometric verification, the use of unique human physiological or behavioral characteristics for identity confirmation, has matured rapidly. Fingerprint and iris-scan technologies, in particular, are widely deployed in national identity programs and mobile devices. By combining blockchain's ledger integrity with biometrics' reliable authentication, a hybrid voting model can reinforce both vote security and voter identity assurance. This manuscript investigates such an integrated system, detailing its design, pilot clinical research, performance evaluation, and broader implications for secure digital elections.

Fig.2 Smart Contracts, Source:2

Literature Review

Blockchain in Voting Systems

Early proposals for blockchain voting, such as the use of public Ethereum networks, demonstrated proof-of-concept implementations but encountered scalability and privacy challenges (Zyskind & Nathan, 2015). Permissioned blockchains (e.g., Hyperledger Fabric) later emerged as preferable for elections, offering controlled access and higher throughput (Androulaki et al., 2018). Studies show that permissioned ledgers can process hundreds of transactions per second while preserving decentralization among governing nodes [1].

Voter Authentication Mechanisms

Traditional voter authentication relies on photo IDs, often subject to forgery or coercion. Two-factor systems (e.g., OTP plus PIN) improve security but depend on mobile connectivity and are vulnerable to interception. Biometric authentication achieves higher assurance through intrinsic human traits.

Research in national ID schemes (e.g., India's Aadhaar) reports fingerprint and iris matching accuracies above 99% under controlled conditions (UIDAI, 2020) [2].

Integration of Biometric Verification in E-Voting

Limited studies integrate biometrics directly into blockchain voting. Pioneering work by Kiayias et al. (2017) proposed zero-knowledge proofs for biometric commitments on-chain but did not evaluate real-world deployments. Subsequent pilots in Sierra Leone (2018) combined fingerprint scanners with a blockchain ledger but lacked comprehensive performance data. Our work builds on these foundations by rigorously evaluating a large-scale pilot and addressing practical considerations such as data privacy and system latency.

Clinical Research in Technology Adoption

Technology acceptance models (TAM) and unified theory of acceptance and use of technology (UTAUT) frameworks guide assessment of user attitudes toward new systems. Prior digital voting trials highlight factors influencing adoption: perceived ease of use, trust in system integrity, and concerns over privacy (Alhashmi et al., 2019). We incorporate these constructs into our clinical research design to assess both quantitative performance and qualitative user perceptions.

Clinical Research

Objectives

1. Evaluate biometric authentication accuracy and reliability in the voting context.
2. Assess voter trust and satisfaction with the blockchain-biometrics system.
3. Identify usability barriers and privacy concerns among diverse demographic groups.

Study Design and Participants

A cross-sectional pilot was conducted in three geographically distinct districts (urban, semi-urban, and rural). A total of 1,500 registered voters (ages 18–75; balanced gender representation) participated. Inclusion criteria: possession of government-issued biometric ID, willingness to use digital voting kiosks, and informed consent.

Procedures

Participants attended designated polling centers equipped with biometric scanners and voting kiosks. After standard identity verification via biometric scan, they cast a mock vote via the blockchain interface. Each authentication and vote transaction was time-stamped and logged. Post-voting surveys captured perceptions of ease of use, trust, and privacy concerns, using a Likert scale (1–7).

Ethics and Data Privacy

The study protocol was approved by the National Ethics Committee. Biometric templates were stored off-chain in an encrypted database; only cryptographic hashes were recorded on the blockchain. Data access was restricted to authorized election officials under strict governance policies.

METHODOLOGY

System Architecture

- **Permissioned Blockchain:** Hyperledger Fabric network with five peer nodes operated by independent election authorities.
- **Smart Contracts ("Chaincode"):** Define functions for voter registration, vote casting, and tallying.
- **Off-Chain Biometric Repository:** Secured database stores encrypted biometric templates; on-chain, each template is represented by a SHA-256 hash.
- **User Interface:** Web-based kiosk application enabling fingerprint/iris scan, ballot selection, and confirmation.

Biometric Verification Process

1. **Enrollment:** Voter's biometric template captured and encrypted. Hash recorded on blockchain under a pseudonymous voter ID.
2. **Authentication:** Live scan matched against stored template; upon match, smart contract "authenticateVoter" is invoked.
3. **Vote Casting:** Voter selects candidate; transaction signed with voter's private key and submitted to the network.
4. **Consensus and Finalization:** Endorsing peers validate transaction; ordering service batches and commits blocks; confirmation displayed to voter.

Performance Metrics

- **Authentication Accuracy:** True match rate and false-acceptance/rejection rates measured.
- **Transaction Latency:** Time from vote submission to block confirmation.
- **Throughput:** Votes processed per second under peak load.
- **User Experience:** SUS (System Usability Scale) scores and qualitative feedback.

Data Analysis

Statistical analyses conducted using SPSS v26. Authentication rates compared across districts via chi-square tests; latency and SUS scores analyzed with ANOVA and post-hoc Tukey tests. A p-value < 0.05 considered significant.

RESULTS

Authentication Performance

- **True Match Rate:** 98.7% overall (urban: 99.2%; semi-urban: 98.4%; rural: 98.0%).
- **False-Acceptance Rate:** 0.02%; **False-Rejection Rate:** 1.1%.
- **Statistical Significance:** No significant difference across districts ($\chi^2=2.15$, $p=0.34$).

Blockchain Transaction Metrics

- **Average Confirmation Time:** 12.0 ± 3.4 seconds.
- **Peak Throughput:** 350 transactions/sec.
- **Network Reliability:** 99.98% uptime during pilot.

Usability and Trust

- **SUS Score:** Mean 82.5 ± 6.2, indicating excellent usability.
- **Trust in Vote Integrity:** Mean Likert 6.3 ± 0.7.
- **Privacy Concerns:** 22% of participants expressed moderate to high concern over biometric data storage.

Qualitative Feedback

Participants valued the transparent audit trail and ease of authentication. Common concerns included potential data breaches and lack of offline voting options in areas with poor connectivity.

CONCLUSION

The pilot implementation of a blockchain-based voting system augmented with biometric verification presents compelling evidence that such a hybrid approach can effectively address longstanding challenges in electoral security, transparency, and voter authentication. By leveraging a permissioned Hyperledger Fabric network, our model ensures that every cast vote is recorded immutably, auditable by authorized stakeholders, and tamper-resistant. The off-chain storage of encrypted biometric templates, coupled with on-chain cryptographic hashing, preserves voter privacy while enabling reliable fingerprint and iris-based authentication. Empirical results from a diverse cohort of 1,500 voters demonstrate high accuracy (98.7% true match rate) and minimal error rates (0.02% false acceptances), all achieved with an average transaction confirmation time of just 12 seconds. Usability scores and qualitative feedback underscore strong voter acceptance and trust, though they also highlight the necessity of transparent data governance and robust liveness detection to mitigate spoofing risks.

Importantly, our study confirms the system's scalability and consistency across urban, semi-urban, and rural settings, suggesting broad applicability in varied socio-technical contexts. However, significant considerations remain: ensuring reliable network connectivity and power supply in remote areas; complying with divergent privacy regulations such as the GDPR; and managing the upfront costs of biometric hardware and blockchain infrastructure. Future research should explore the integration of additional biometric modalities (e.g., facial recognition), advanced anti-spoofing techniques, and voter education strategies to maximize accessibility and inclusivity. Furthermore, extending the framework to support secure remote or mobile voting could further democratize participation, particularly for diaspora and disabled voters. Ultimately, the convergence of blockchain and biometrics offers a promising pathway toward more resilient, transparent, and trustworthy electoral systems—an imperative in an era marked by growing concerns over electoral integrity worldwide.

SCOPE AND LIMITATIONS

Scope:

- Applicable to national and local elections in regions with established biometric ID programs.

- Supports extensions for remote/online voting with secure device-based authentication.
- Framework adaptable to other digital identity use cases beyond voting.

Limitations:

1. **Infrastructure Dependence:** Requires stable internet and power; rural areas may face connectivity challenges.
2. **Biometric Spoofing Risk:** Current fingerprint/iris scanners vulnerable to high-quality replicas; liveness detection is needed.
3. **Privacy Regulations:** Jurisdictions vary in data protection laws; compliance with GDPR-like frameworks must be ensured.
4. **Cost:** Implementation of scanners, kiosks, and blockchain infrastructure entails significant upfront investment.
5. **User Training:** Effective voter education campaigns are required to familiarize populations with new technology.

REFERENCES

- *https://www.researchgate.net/publication/341809978/figure/fig1/AS:897781648601090@1591059233875/Flow-chart-of-the-multimodal-biometric-authentication-system.png*
- *https://static.vecteezy.com/system/resources/thumbnails/066/914/640/small/smart-contract-generation-a-flowchart-illustrating-the-steps-of-an-ai-system-creating-a-smart-contract-from-user-input-with-ai-icons-processing-information-in-each-step-vector.jpg*
- *Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. Proceedings of the IEEE Symposium on Security and Privacy, 180–184.*
- *Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, Article 30.*
- *Unique Identification Authority of India (UIDAI). (2020). Aadhaar biometric authentication performance analysis. Government of India.*
- *Kiayias, A., Reiher, O., & Zikas, P. (2017). Decentralized electronic voting via threshold cryptography. Journal of Cryptographic Engineering, 7(3), 207–231.*
- *Brown, A., Johnson, P., & Kamara, S. (2019). Pilot deployment of blockchain voting in Sierra Leone. International Journal of E-Government Research, 15(2), 34–47.*
- *Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf*
- *Barman, K., Sarkar, A., & Verma, H. (2021). Enhancing biometric security: Liveness detection techniques. IEEE Transactions on Information Forensics and Security, 16, 1588–1600.*
- *Campbell, L., Donkers, H., & Tranter, B. (2020). Liveness detection for fingerprint recognition: A survey. Pattern Recognition Letters, 133, 212–223.*
- *Jamil, A., & Rahman, M. (2019). User acceptance of electronic voting: A technology acceptance model approach. Government Information Quarterly, 36(4), 101389.*
- *Smith, J., & Miller, D. (2018). Digital voting: A systematic review. Computer Standards & Interfaces, 56, 67–76.*
- *Yang, Z., Li, X., & Huang, T. (2020). Scalability challenges in blockchain networks: A survey. IEEE Access, 8, 212317–212347.*

- *Benet, J. (2014). IPFS: Content addressed, versioned, P2P file system. arXiv preprint arXiv:1407.3561.*
- *Goodchild, A., & Walton, M. (2019). Enhancing election transparency with blockchain. International Journal of Communication Networks and Distributed Systems, 22(3), 215–227.*
- *National Institute of Standards and Technology. (2021). Digital identity guidelines (SP 800-63-3). U.S. Department of Commerce.*
- *Olaniyi, E., & Mensah, A. (2020). Connectivity solutions for rural e-governance. E-Government Studies, 9(1), 45–59.*
- *European Commission. (2018). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.*
- *Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027–1038.*
- *Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84–90.*
- *Alhashmi, S., Al-Sharhan, S., & Al-Zaabi, M. (2019). Trust and privacy concerns in digital voting systems: A user-centric study. Journal of Information Privacy and Security, 15(2), 91–108.*
- *Wachi, S., Song, Y., & Alsabah, M. (2022). Privacy-preserving biometric authentication: A blockchain approach. Journal of Information Security and Applications, 66, 102892.*