Blockchain-Based Voting System Using Biometric Authentication

Payal Ramesh lad[1], Prof. S. V. Raut[2]
Department of Computer Science and Engineering, DRGIT&R College of Engineering Amravati

***Abstract*—We propose a secure electronic voting framework that combines blockchain and biometric identification to ensure transparent, tamper-resistant elections. In this system, each eligible voter is registered with a unique biometric identity (e.g. fingerprint or facial scan) linked to a blockchain account. During voting, the voter authenticates via their biometric and casts a vote transaction on the blockchain. The decentralized ledger immutably records votes and prevents unauthorized tampering Biometric verification ensures one-person-one-vote and protects against impersonation. We detail the system architecture (user registration, authentication, vote casting and tallying) and analyze its security, highlighting how blockchain's transparency and cryptographic guarantees, combined with biometric safeguards, address key election integrity challenges. The proposed design is novel in integrating end-to-end encryption of ballots with biometricbased voter admission, offering verifiability and privacy simultaneously.**

***Index Terms*—Blockchain; Electronic voting; Biometric authentication; Security; Decentralization; Transparency**

1. INTRODUCTION

Modern elections demand trust, security, and transparency. Traditional paper ballots are trusted but slow and costly, while electronic voting machines (EVMs) and online systems introduce risks of hacking, manipulation, and fraud. Centralized voting systems suffer from single points of failure and require voters to trust authorities. Blockchain technology, with its decentralized and tamper-evident ledger, has emerged as a promising solution for secure voting. Each vote can be treated as a transaction on a distributed ledger, ensuring that once recorded it cannot be altered or deleted.

However, a key challenge is authenticating voters securely yet anonymously. Biometric authentication (e.g. fingerprint, iris or facial recognition) provides a strong way to bind a voter's identity to their vote without relying on passwords or tokens. By integrating biometrics, the system verifies the voter's identity at login and ensures only registered voters can submit ballots. Crucially, combining biometrics with blockchain balances integrity and privacy: the blockchain records an immutable vote, while the biometric check prevents impersonation.

This paper describes a novel blockchain-based voting system secured by biometric authentication. We design the protocol steps (registration, voting, consensus, tallying), illustrate the system architecture, and discuss how security properties are achieved. Our contributions include a unique integration of onchain vote recording with off-chain biometric verification, a method for one-time voter registration, and an analysis of attack resistance. By leveraging both technologies, the system ensures that each registered voter casts exactly one vote (authenticated biometrically) and that all votes are publicly verifiable on a blockchain, enhancing election transparency while preserving voter privacy.

2. BACKGROUND AND RELATED WORK

2.1. Blockchain in E-Voting

Blockchain has become widely studied for electronic voting due to its security properties. In a blockchain election, votes are recorded as transactions in blocks that are chained by cryptographic hashes. This provides decentralization (no single authority controls the ledger) and immutability (past transactions cannot be retroactively changed). As Jafar *et al.* note, blockchain's decentralization and non-repudiation make it an attractive replacement for conventional e-voting, potentially reducing costs and fraud. Multiple survey papers report that blockchain can eliminate the need for a central tallying authority and provide end-to-end verifiability of results. For example, every vote transaction can be cryptographically signed and later

audited, ensuring transparency. However, blockchain alone does not solve all problems: privacy and scalability remain challenges, and additional measures (like encryption or mix-nets) are often needed in practice.

Many prototype systems and research frameworks exist. Some real-world trials have used custom blockchains for voting. Platforms like Voatz (used in some U.S. elections) employ blockchain ledgers behind the scenes to record votes in a way that is auditable. The Voatz system in particular authenticates voters via smartphone biometric scans (fingerprint or retina) and then logs votes on a blockchain. Such examples illustrate the feasibility of blockchain voting but also highlight the need for strong voter authentication and careful UX design.

2.2. Biometric Authentication in Voting

Biometric methods (fingerprint, iris, face) have been studied as a solution for voter identity verification. Unlike passwords or tokens, biometrics are unique to each individual. Prior work has used fingerprint readers on voting machines to authenticate voters at the polling station. Biometric keys can also be used to generate cryptographic keys, tying a vote transaction to a physical person without revealing identity. Research (e.g., Olaniyi *et al.* 2016) demonstrated block diagrams of fingerprint-based e-voting modules, ensuring only registered fingerprints unlock the system. Reviews on e-voting security stress that adding biometric checks can greatly reduce impersonation and double-voting.

However, storing biometric data raises privacy concerns. In our system, biometrics are used only at registration (to establish a

voter identity) and for local authentication on the user's device. No raw biometric template is published on-chain. Instead, the blockchain contains only pseudonymous voter IDs and encrypted vote data. This follows best practices from related research: as one analysis points out, distributing biometric data across nodes on a blockchain (rather than centralized) further enhances security and privacy.

2.3. Hybrid Approaches and Gaps

Some existing proposals integrate biometrics and blockchain. For example, Adeniyi *et al.* (2024) describe using biometric readings to generate voters' cryptographic keys in a blockchain-based voting scheme. Security reviews note that combining blockchain with biometric authentication is powerful because it simultaneously addresses trust (blockchain ledger) and identity (biometrics) issues. Despite these advances, there is limited open literature on complete end-toend designs that can be directly used by election

authorities. Many studies focus on components or algorithms, but do not tie them together in a full system model. Our work fills this gap by detailing a comprehensive architecture with an emphasis on practicality: we assume voters have a personal device (smartphone or kiosk) capable of biometric scanning, and we use an existing public blockchain or consortium chain for recording votes.

3. SYSTEM DESIGN

3.1. Overview

The proposed system has three main phases: (1) Voter Registration, (2) Vote Casting, and (3) Verification. Figure 1 (conceptual) illustrates the architecture. Key entities include the *Election Authority (EA)*, *Voters*, *Biometric Authentication Module*, and a *Blockchain Network* (with validator nodes). The EA is responsible for initial voter enrollment and initializing election parameters on-chain; Voters participate by authenticating and casting ballots; Validators (miners or nodes) add vote transactions to blocks.

During Registration, each voter's identity is validated by the election authority (e.g. via government ID) and linked to a unique blockchain account. At this time, the voter's biometric template (fingerprint, face, etc.) is captured by a secure on-site device and encoded (or used to generate a public/private key pair). The EA stores a cryptographic hash of the voter's biometric-encrypted key to enable later authentication, without revealing the raw data. The voter account (public key or address) is whitelisted for this election and recorded on-chain. Importantly, at no point are actual biometric scans stored on the public ledger only hashed credentials or proofs, as shown in prior secure e-voting schemes.

Vote Casting proceeds as follows. Each voter uses the official voting app or terminal. The voter signs in by scanning their biometric (e.g. fingerprint). A local authentication module on the device compares this scan against the voter's registered template. If it matches, the voter is unlocked and allowed to vote.

The voter then selects their choices, which are encrypted on-device to preserve privacy. The device constructs a vote transaction: it includes the voter's (pseudonymous) account, the encrypted ballot, and a digital signature (based on the voter's private key derived during registration). This signed transaction is broadcast to the blockchain network. Validator nodes verify that the signature is valid and that the voter has not yet voted (enforcing one-vote-per-account). Valid transactions are grouped into a block and appended to the chain by consensus (e.g. Proof-of-Work or Proof-of-Stake). Because of the underlying blockchain, all transactions (votes) are immutable and timestamped.
Tallying and Verification can occur in two ways. If ballots are encrypted with a public key whose private key is held in a secure multiparty or threshold manner, validators or a predefined party can jointly decrypt votes after voting ends, tallying results transparently. Alternatively, votes could be recorded in a homomorphically encrypted form allowing public aggregation without decryption of individual ballots. In either case, anyone can audit the blockchain to verify the integrity of the election: they see every vote transaction counted exactly once, and the cryptographic proofs ensure no tampering. Importantly, votes remain secret throughout the process,

linking only to pseudonymous IDs. At the end, the election result is published, and voters can optionally verify that their vote was counted (e.g. by checking a receipt or seeing their hash on a public bulletin board) without revealing their selection to others.

3.2. Key Procedures and Security Measures

1. Voter Enrollment :

The election authority verifies voter eligibility off-chain. Upon approval, the voter's unique ID is created as a blockchain address. The voter provides a biometric sample, which the system uses to generate a cryptographic key pair or to encrypt a randomly generated key. A commitment of this biometricderived key is recorded on-chain along with the voter's public address, without revealing the raw biometric data. This ties the voter's identity to a blockchain account.

2. Authentication

When casting a vote, the voter uses a biometric scanner (smartphone sensor or kiosk). The fresh biometric scan is processed locally: it must match the stored template from registration. This step prevents stolen credentials – even if someone copied the voter's blockchain address, they cannot use it without the biometric. No biometric data leaves the local device; only a "yes/no" pass outcome. In this way, *identity theft* and multiple voting are prevented by linking the vote to a biological trait.

3. Ballot Casting and Encryption:

Once authenticated, the voter fills out their ballot. The selections are encrypted immediately on the device (for privacy) using the election's public key scheme. This encrypted ballot, along with the voter's address and a timestamp, form a transaction. The device signs this transaction with the voter's private key (from registration). The signed, encrypted vote is submitted to the network.

4. Consensus and Ledger Entry:

Blockchain validator nodes receive incoming vote transactions. Each node checks the digital signature against the voter's address and confirms that this voter account has not already cast a vote (using the blockchain's history). Valid votes are included in the next block according to the network's consensus (e.g. proof-of-work or proof-ofstake). Because every block is chained cryptographically, any attempt to alter past votes (for fraud) would be immediately evident and rejected by

These procedures collectively provide strong security guarantees. Integrity is achieved through the blockchain's cryptographic linking of blocks and digital signatures: votes cannot be changed or forged once on-chain. Authentication is enforced by biometrics: even if an attacker obtains a voter's private key, they cannot use it without the voter's fingerprint or face, preventing *double-voting* and *masquerade* attacks. Transparency comes from the public ledger – anyone can audit the election log to confirm that the total votes equal the sum of individual ballots. Privacy is maintained because ballots are encrypted and voter accounts are pseudonymous; only the fact of "an eligible voter cast a ballot" is public, not the vote content.

3.3. Advantages Over Traditional Systems

Our design addresses major challenges of electronic voting. By eliminating central authorities (through

decentralization), we remove the risk of insider tampering or single-point failures. The blockchain ledger provides an indelible audit trail of votes. Biometric authentication ensures that votes are tied to real individuals without needing vulnerable ID cards or shared credentials. For example, smartphone-based voting apps with fingerprint login have demonstrated that convenient biometric voting is feasible. Furthermore, our system can be made scalable: an efficient consensus (or a consortium blockchain) can handle large electorates with minimal delay. In terms of user experience, voters merely authenticate and cast ballots as usual, but with stronger security under the hood.

Overall, by combining blockchain's immutability and distributed trust with biometric unique identity verification, the system ensures one-person-one-vote in an end-to-end verifiable manner. It resists common attacks (vote alteration, ballot stuffing, identity fraud) while potentially increasing voter confidence through greater transparency.

4. CONCLUSION

We have outlined a comprehensive blockchain-based voting framework secured by biometric authentication. The proposed system leverages a public ledger to record each vote immutably and transparently, while using fingerprint/iris scans (or other biometrics) to authenticate voters at the point of entry. This dual approach enhances security: the blockchain ensures tamperproof recording of ballots, and biometrics guarantee that only legitimate voters participate. Compared to purely paper or electronic methods, our design offers strong auditability and end-to-end security.

While promising, practical deployment requires further work on usability, legal frameworks, and privacy safeguards. Future enhancements could include multi-factor biometrics, robust key recovery methods, and formal verification of the protocol.
Nonetheless, the combination of decentralized blockchain.Infrastructure with biometric-based voter identity presents a unique, near-future-ready solution to strengthen democratic voting processes.

REFERENCES

[1] Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Jafar, M., Aziz, M., "Blockchain-Based E-Voting Systems: A Technology Review," MDPI Electronics, vol. 10, no. 5, 2021. [Online]. Available: https://www.mdpi.com/2079-9292/10/5/584

[3] Sharma, S., Singh, A., "Biometric Authentication in Secure Voting Systems," International Research Journal of Engineering and Technology (IRJET), vol. 12, no. 2, 2023. [Online]. Available: https://www.irjet.net/archives/V12/i2/IRJETV12I288.pdf

[4] Spanos, A., Kantzavelou, I., "BieVote: Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework," ResearchGate, 2022. [Online]. Available: https://www.researchgate.net/publication/357861285 _BieVote_A_Biometric_Identification_Enabled_ Blo ckchain-Based_Secure_and_Transparent_Voting_Framework

[5] Adeniyi, O., Olaniyi, O., "Integration of Blockchain and Biometrics in Secure E-Voting Systems," International Journal of Computer Applications, vol. 176, no. 31, 2024.

[6] Voatz, "Blockchain Mobile Voting App Overview," Voatz White Paper, 2020. [Online]. Available: https://voatz.com/resources/

[7] Olaniyi, O., Adeniran, F., "Fingerprint-Based Biometric Authentication in Electronic Voting Systems," International Journal of Information Security and Privacy, vol. 10, no. 4, pp. 45–59, 2016.