IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

AI-Enhanced Blockchain Voting Platform with Multi-Factor Biometric Authentication

Aadesh V. R.[1], Aswin K. R.[2], Kasinath N. B.[3], Akshay N. K.[4], Ms. Sabitha C. B.[5], Ms. Anjitha P.[6]
Department of Computer Science and Engineering[1,2,3,4]
Assistant Professor, Department of Computer Science and Engineering[5]
Assistant Professor, Department of Computer Science and Engineering[6]
Thejus Engineering College, Thrissur, Kerala, India

Abstract: *Electronic voting can improve the accessibility and speed of election workflows, but remote voting introduces challenges involving voter impersonation, repeated voting, centralized record manipulation, limited voter-side confirmation, and the protection of sensitive identity data. This paper presents the design of an AI-enhanced blockchain voting platform that combines a Flutter mobile application with a Python backend, phone-number one-time-password (OTP) verification, device-mediated fingerprint authentication, facial verification with liveness checking, smart-contract-based vote validation, and a blockchain-backed audit record. The proposed workflow guides a voter through OTP verification, fingerprint approval, live facial verification, ballot submission, and receipt generation. During the voting session, the camera and recording service are intended to remain active; security, camera, authentication, or network failures terminate the session and return the user to login. The architecture separates the mobile interface, verification services, backend, application database, smart-contract layer, and ledger. We also identify design constraints that are essential for a credible voting system, particularly ballot secrecy, biometric-data minimization, secure off-chain storage, recording consent and retention, and the distinction between tamper-evident records and end-to-end election verifiability. This is a proposed system design; implementation results and performance measurements are not claimed.*

Keywords: Electronic voting, blockchain, multi-factor authentication, one-time password, fingerprint authentication, facial recognition, liveness detection, smart contract, auditability

I. INTRODUCTION

Voting systems must protect voter eligibility, ballot integrity, ballot secrecy, and the legitimacy of the final tally. Paper-based elections and electronic voting machines provide established procedures, but they still rely on physical access, administrative processes, and controls that may be difficult to extend to remote or mobile voting. Online voting can reduce access barriers, yet it also expands the attack surface: credentials can be stolen, voters can be impersonated, centralized records can be modified, and a voter may have little independent evidence that a submitted ballot was accepted.

Blockchain has been studied as a way to make election records auditable and resistant to undetected modification. However, an immutable ledger alone does not establish that the person submitting a ballot is eligible, that the input was captured correctly, or that a published tally preserves ballot secrecy. Surveys of blockchain-based voting systems identify unresolved issues involving privacy, scalability, governance, usability, and verifiability [15], [16]. Research on voter trust also emphasizes that technical assurances must be accompanied by institutional confidence and understandable procedures [1].

This paper describes a proposed mobile voting platform intended to address several of these concerns through multiple authentication factors and a ledger-backed voting workflow. The design uses a Flutter application, a Python service layer, phone-number OTP verification, device fingerprint authentication, facial matching with liveness checking, a

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, November 2026 Impact Factor: 8.2

smart contract to reject repeat voting, and receipt generation after transaction confirmation. The camera-recording requirement in the project concept is treated as a session-monitoring function, with associated privacy safeguards discussed explicitly.

The contributions of this paper are: 1) a layered architecture integrating mobile voting, authentication, biometric verification, backend controls, and blockchain recording; 2) a five-stage voter workflow with automatic session termination on specified failures; and 3) a discussion of design safeguards needed to avoid conflating ledger immutability with voter anonymity, biometric privacy, or election correctness.

II. LITERATURE SURVEY

Existing work can be grouped into blockchain voting architectures, biometric voter verification, and broader security and trust analyses. Blockchain-oriented surveys classify voting designs by their consensus, smart-contract, privacy, and verification properties [15], [16]. Earlier prototypes such as EtherVote explore Ethereum-based eligibility and ballot processing [17], while ElectionBlock examines fingerprint-assisted blockchain voting [19]. R. Vittal's blockchain voting application and other early prototypes similarly investigate how distributed ledgers may support auditable voting records [20]. These studies motivate a ledger layer but also show that transaction immutability is only one part of election security.

Several studies combine blockchain with biometric authentication. Faruk et al. describe an online voting architecture using blockchain with fingerprint and facial recognition, including a Hyperledger Fabric design [4]. DemocracyGuard combines Ethereum smart contracts with facial recognition [8]. Ibrahim et al. propose ElectionBlock with fingerprint authentication [19], while Pooja et al. examine deep-learning-based face detection in a coercion-resistant blockchain voting design [9]. Other work considers biometric authentication with blockchain and watermarking [14], facial-recognition-based e-voting [10], and AI-supported facial verification [13]. These approaches demonstrate the relevance of biometrics but differ in authentication factors, deployment assumptions, and privacy mechanisms.

Multi-modal authentication and privacy are also recurring themes. Ahmadieh and El Madhoun compare multi-modal authentication approaches for e-voting [5]. Osayomore et al. study a blockchain design using fingerprint and facial recognition [12], while Kumar et al. examine blockchain, biometrics, and zero-knowledge proofs as a combined approach [11]. A quantum-secure framework proposes post-quantum signatures alongside biometric validation [3]. A separate student-project proposal listed by KSCST considers face and fingerprint authentication for blockchain voting; it is a project proposal rather than a peer-reviewed article [6]. The source presentation also includes work on blockchain voting with biometric authentication [7], online voting with face recognition [10], and a 2026 IRJET system proposal [18].

The reviewed literature further includes a systematic review of blockchain e-voting solutions [16], a survey of blockchain voting [15], and studies of system acceptance and trust [1], [2]. The cited works collectively indicate that authentication, transparent record keeping, privacy, usability, and trust must be considered together. The proposed platform builds on these themes by combining OTP, device-mediated fingerprint approval, facial liveness verification, smart-contract checks, session monitoring, and a voter receipt. Its key distinction is the intended combination of three verification factors with a continuous session-monitoring workflow; its feasibility and privacy properties still require implementation and evaluation.

III. SYSTEM DESIGN

Design Objectives

The design is guided by six objectives: (i) authenticate a voter through independent factors; (ii) prevent a voter from casting more than one ballot in an election; (iii) maintain a tamper-evident record of accepted voting transactions; (iv) provide a receipt after successful submission; (v) monitor the active voting session and terminate it on defined failures; and (vi) minimize exposure of biometric and personally identifying information.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

Architecture

The architecture contains a voter application, OTP service, Python backend, biometric verification service, application database, election-management smart contract, blockchain ledger, video-recording service, and security/error handler. The Flutter application provides login, voting, and view-only profile screens. The OTP service verifies the phone number. After OTP approval, the application requests device fingerprint authentication and performs live facial verification with a liveness check. The Python backend coordinates authentication, voting requests, storage, monitoring, and error handling. The smart contract validates eligibility and the one-vote rule before the transaction is committed to the ledger.

Fig. 1 reproduces the high-level architecture from the project presentation. The original presentation identifies Hyperledger Fabric or an Ethereum test network as blockchain alternatives, SQLite or Firebase as database alternatives, and FastAPI or Flask as backend alternatives. These are candidate technologies, not final implementation choices. The diagram also depicts biometric and profile data in a database and hashed or encrypted records on the ledger; the final implementation must define the exact data schema and trust boundaries before deployment.

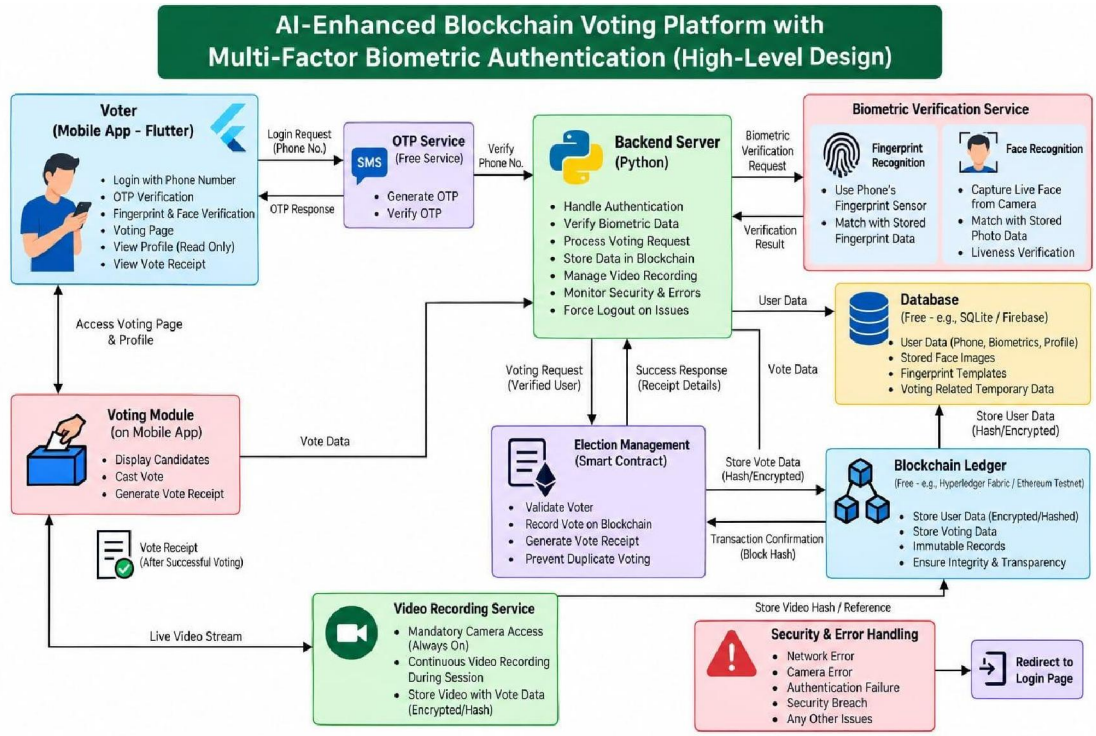


Fig. 1. High-level architecture of the proposed AI-enhanced blockchain voting platform, adapted from the project presentation.

Voter Authentication and Voting Workflow

The voter workflow consists of five sequential stages:

1) *Phone and OTP:* The voter enters a registered phone number. An OTP service generates and verifies a one-time code before the application proceeds.

2) *Fingerprint approval:* The application invokes the device's biometric authentication interface. The operating system should perform the fingerprint match and return an authentication result to the application; raw fingerprint templates should not be exposed to the app or transferred to the backend.

3) *Facial verification:* The front camera captures a live face sample. The verification service compares it with an enrolled reference and performs a liveness check to reduce simple photo or screen-replay attacks. The project

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

presentation lists OpenCV, face-recognition libraries, and ML Kit as possible implementation choices; a final model and threshold remain to be selected.

4) *Vote submission:* After all authentication checks pass, the voting module displays the candidates and accepts one selection. The backend submits a transaction to the election smart contract. The contract checks that the voter is eligible and has not already voted, then records the accepted ballot transaction.

5) *Receipt:* After transaction confirmation, the application generates a receipt for the voter. The receipt should prove that a transaction was accepted without exposing the voter's candidate selection or creating a public link between the voter and the ballot.

Backend, Ledger, and Data Handling

The Python backend coordinates OTP status, biometric-verification outcomes, voting requests, camera-session status, and transaction responses. The application database is intended to retain user profiles and the minimum information needed for enrollment and verification. The blockchain layer is intended to provide an immutable or tamper-evident record of accepted transactions and integrity references. The project presentation proposes storing hashed or encrypted data on the ledger and lists Hyperledger Fabric and Ethereum testnet as alternatives.

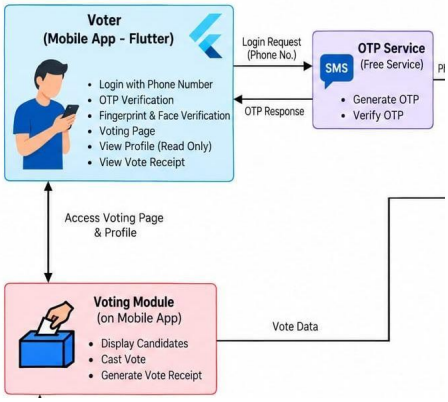


Fig. 2. Voter mobile application and OTP interaction shown in the project design.

For a privacy-preserving design, raw face images, video files, and biometric templates should not be written directly to a public or broadly replicated ledger. They should remain in encrypted, access-controlled off-chain storage with a defined retention period. The ledger can store cryptographic commitments, transaction identifiers, election identifiers, and a one-time eligibility-spent state. In particular, the mapping between a voter's real identity and the selected candidate must not be publicly readable. A design that writes voter identity and ballot choice together would undermine ballot secrecy even if the record were immutable. The architecture therefore requires a separation between identity verification and anonymous ballot recording, potentially using unlinkable credentials or another privacy-preserving authorization mechanism in a later implementation.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

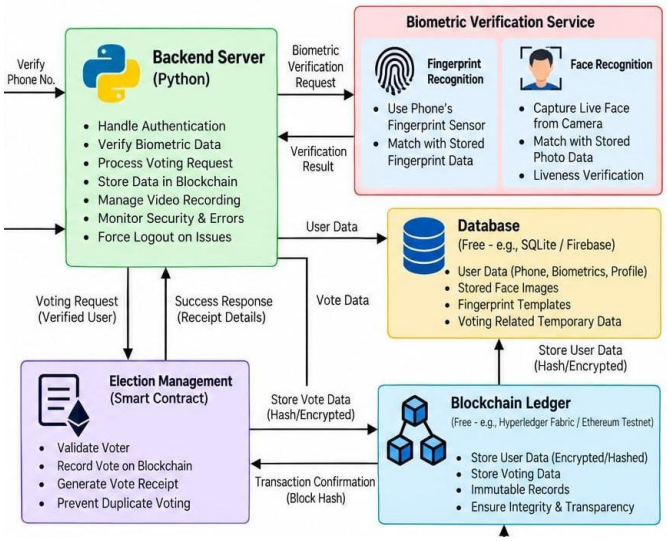


Fig. 3. Backend, biometric verification, database, and blockchain components.

Session Monitoring and Failure Handling

The project design specifies continuous camera access and video recording from login until a receipt is issued. The recording service supplies a video reference or hash to the ledger, while the security handler monitors network errors, camera failures, authentication failures, and other security conditions. If any such failure occurs, the session is terminated and the user is redirected to the login page, as shown in Fig. 4.

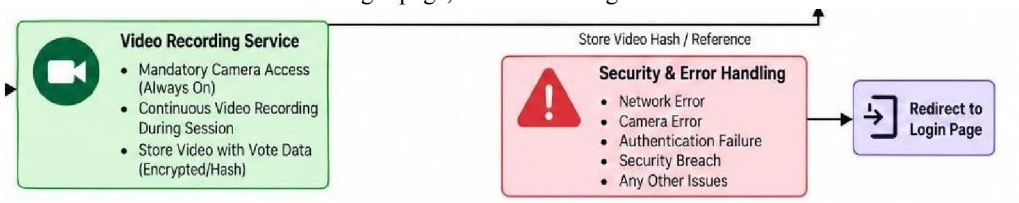


Fig. 4. Continuous session-recording concept and automatic logout on security or operational errors.

A hash can help detect later modification of a retained video file, but it does not prove that the camera captured the complete session or that the recording is free from gaps. Continuous recording also introduces privacy, surveillance, storage, and data-protection risks. A real deployment would require a clear purpose, lawful basis and informed notice, strict access controls, encryption, audit logging, short retention, and a process for handling user complaints. The system must not treat recording alone as proof that a vote was voluntary or free from coercion.

Security Properties and Open Design Decisions

Table I summarizes the intended controls and the issues that remain to be resolved. OTP, fingerprint approval, and face verification provide layered authentication, but none guarantees eligibility by itself. OTP depends on the security of the phone-number channel and service provider. Device fingerprint authentication depends on the integrity of the operating system and enrolled device. Facial recognition depends on capture quality, liveness performance, demographic variation, and secure enrollment. Smart contracts reduce the scope for unauthorized state changes only when their logic, access-control rules, and deployment process are audited.

TABLE I: Design Controls and Remaining Risks

Control	Purpose and remaining consideration
OTP	Confirms control of a registered phone number; vulnerable to SIM-swap, interception, and service outages.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, November 2026 Impact Factor: 8.2

Control	Purpose and remaining consideration
Device fingerprint	Adds a local biometric factor; the app should receive only a success/failure result, not raw templates.
Face and liveness	Checks the live user against an enrolled reference; requires bias, spoofing, and false-rejection evaluation.
Smart contract	Enforces eligibility and one-vote state; needs independent code review and governance controls.
Ledger hashes	Supports integrity checking; does not by itself provide ballot secrecy or end-to-end verifiability.
Session recording	Supports incident review; needs consent/notice, retention limits, encryption, and access auditing.

IV. CONCLUSION AND FUTURE WORK

This paper has presented the design of a mobile blockchain voting platform that combines phone-number OTP verification, device-mediated fingerprint authentication, facial verification with liveness checking, smart-contract validation, session monitoring, and receipt generation. The proposed architecture uses a Flutter voter application, a Python backend, an application database, a biometric verification service, and a blockchain ledger. Its intended workflow is to authenticate the voter in stages, permit one accepted ballot per eligible voter, record a transaction, and return a receipt to the user.

The design remains conceptual and has not been validated through a working prototype or a controlled evaluation. Several decisions must be completed before implementation, including the final backend framework, blockchain network, database, face model, liveness method, smart-contract interface, and off-chain data-retention strategy. Future work should implement a prototype and evaluate OTP delivery, biometric false-acceptance and false-rejection rates, spoof resistance, transaction latency, concurrent voting load, fault recovery, and accessibility. Security analysis must also test ballot secrecy, identity–vote unlinkability, smart-contract correctness, key management, and the possibility of coercion or device compromise. Finally, the continuous-recording requirement must undergo privacy and legal review. These evaluations are necessary before the platform can be considered suitable beyond a controlled academic demonstration.

REFERENCES

1. C. C. Wermelinger, A. M. Mariano, and J. M. da Silva, “Trust and Security in Critical Digital Infrastructures: A Conditional Analysis of Acceptance and Intention to Change in Electronic Voting Systems,” *IEEE Access*, early access, 2026, doi: 10.1109/ACCESS.2026.3676076.
2. Sah, A. Kumar, and B. Bhushan, “Leveraging Blockchain Technology for Secure Online Voting Systems: A Comprehensive Review,” *Journal of Mobile Multimedia*, vol. 21, nos. 3–4, pp. 535–554, 2025, doi: 10.13052/jmm1550-4646.213412.
3. Poudel, U. Poudel, D. Aryal, A. Nepal, P. Pathak, and S. V. Subramaniyaswamy, “A Quantum-Secure and Blockchain-Integrated E-Voting Framework with Identity Validation,” arXiv:2511.16034, 2025.
4. M. J. H. Faruk, F. Alam, M. Islam, and A. Rahman, “Transforming online voting: A novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency,” *Cluster Computing*, vol. 27, pp. 4015–4034, 2024, doi: 10.1007/s10586-023-04261-x.
5. E. Ahmadieh and N. El Madhoun, “Comparative E-Voting Security Evaluation: Multi-Modal Authentication Approaches,” in *Proc. 6th Int. Conf. Blockchain Computing and Applications (BCCA)*, 2024, doi: 10.1109/BCCA62388.2024.10844450.
6. Sushmitha C., Nayana M., Priya B. R., and Srujana S., “Blockchain-Based Biometric Voting System Using Face and Fingerprint Authentication for Secure and Transparent Elections,” 49th Series Student Project

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, November 2026
Impact Factor: 8.2

Programme, Karnataka State Council for Science and Technology, proposal 49S_BE_2385, 2025–2026. (Project proposal; not a peer-reviewed paper.)

7. M. M. da Silva, A. A. A. Silva, N. F. Junior, E. T. Ueda, F. D. Perreira, A. S. dos Santos, A. E. Guelfi, and S. T. Kofuji, "A Proposed Blockchain-Based Voting System with User Authentication through Biometrics," *Enigma – Journal of Information Security and Cryptography*, vol. 8, no. 1, 2021, doi: 10.17648/jisc.v8i1.78.
8. M. S. Peelam, G. Kumar, K. Shah, and V. Chamola, "DemocracyGuard: Blockchain-based secure voting framework for digital democracy," *Expert Systems*, vol. 42, no. 2, Art. no. e13694, 2025, doi: 10.1111/exsy.13694.
9. S. Pooja, L. K. Raju, U. Chhapekar, and C. B. Chandrakala, "Face Detection using Deep Learning to ensure a Coercion Resistant Blockchain-based Electronic Voting," *Engineered Science*, vol. 16, pp. 341–353, 2021, doi: 10.30919/es8d585.
10. V. Khalate, S. A. Dabhade, A. Sawant, S. Paygude, and V. Tarange, "Online Voting System using Face Recognition and Blockchain," *International Research Journal of Engineering and Technology*, vol. 12, no. 6, Jun. 2025.
11. N. Kumar, S. Kumar, A. Waqar, and C. F. Y. Ngantung, "Modernizing Voting Systems: A Comprehensive Approach Using Blockchain, Biometrics and Zero Knowledge Proofs," *International Journal of Electrical, Computer, and Biomedical Engineering*, vol. 3, no. 3, pp. 598–619, 2025, doi: 10.62146/ijecbe.v3i3.116.
12. E. G. Osayomore, O. P. Ejenarhome, and G. P. Oise, "Evaluation of Electronic Based Voting System and Design of Block-Chain-Based Electronic Voting System Enhanced with Fingerprint and Facial Recognition Technologies to Address Impersonation," *FUDMA Journal of Sciences*, vol. 9, no. 7, pp. 13–25, 2025, doi: 10.33003/fjs-2025-0907-3701.
13. X. Pasha and H. Jahankhani, "Securing E-Voting Authentication: A Framework Integrating AI-Based Facial Recognition," in *Sentinels of Cyberspace*, Springer, 2024, pp. 19–46, doi: 10.1007/978-3-031-72821-1_2.
14. A. Ahmed and N. H. M. Ali, "Secure E-voting authentication system employing biometric technology, Crypto-Watermarking Approach and blockchain technology: A Review," *Mustansiriyah Journal of Pure and Applied Sciences*, vol. 3, no. 2, pp. 135–152, 2025, doi: 10.47831/mjpas.v3i2.324.
15. M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," *IEEE Access*, vol. 11, pp. 23293–23308, 2023, doi: 10.1109/ACCESS.2023.3253682.
16. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 70746–70759, 2022, doi: 10.1109/ACCESS.2022.3187688.
17. Spanos and I. Kantzavelou, "A Blockchain-based Electronic Voting System: EtherVote," arXiv:2307.10726, 2023.
18. S. Vinayashree, K. A. Darshan, V. Adithya, G. A. Sandesh, and M. R. Harish Gowda, "Blockchain based Electronic Voting System," *International Research Journal of Engineering and Technology*, vol. 13, no. 5, May 2026.
19. M. Ibrahim, K. Ravindran, H. Lee, O. Farooqui, and Q. H. Mahmoud, "ElectionBlock: An Electronic Voting System Using Blockchain and Fingerprint Authentication," in *Proc. IEEE 18th Int. Conf. Software Architecture Companion (ICSA-C)*, 2021, doi: 10.1109/ICSA-C52384.2021.00033.
20. R. Vittal, "Voting Application using Blockchain Technology," *International Journal for Research in Applied Science and Engineering Technology*, vol. 7, no. IX, pp. 777–782, Sep. 2019, doi: 10.22214/IJRASET.2019.9105