Secure Blockchain E-Voting with Anti-Spoofing and ZK Proofs

Akanksha Mane[1], Poonam Todkar[2], Arpita Patil[2]

[1]*Students, Department of Information Technology, Yadavrao Tasgaonkar College of Engineering & Management*

[2]*Students, Department of Information Technology, Yadavrao Tasgaonkar College of Engineering & Management*

Abstract: Ensuring the integrity, privacy and accessibility of electoral system remains a critical global challenge. This paper proposes a secure blockchain based e-voting framework enhanced with anti-spoofing facial recognition for voter authentication and zero-knowledge proofs to preserve voter anonymity while enabling verifiable results. The proposed system integrates seamlessly with existing election infrastructure, allowing transparent vote recording on a tamper-resistant distributed ledger while preventing identity fraud through advanced biometric anti-spoofing techniques. Zero Knowledge Proofs enable vote verification without revealing individual choices, ensuring both privacy and trust. By combining blockchain's immutability, biometric security and cryptographic privacy guarantees, this approach addresses vote tampering, impersonation, and transparency concerns, offering a scalable , auditable, and privacy-preserving solution for modern elections.

Keywords: *Blockchain, E-Voting, Anti-Spoofing, Facial Recognition, Zero Knowledge Proofs, Election Security, Privacy preserving systems.*

I. INTRODUCTION

The free, fair, and transparent elections are the cornerstone of democratic societies, yet contemporary voting systems continue to suffer from a range of well-documented problems. Physical and electronic processes remain vulnerable to ballot tampering, chain-of-custody failures, duplicate or fraudulent registrations, and impersonation at polling locations. At the same time, many electronic voting proposals trade privacy for verifiability or vice-versa: systems that provide strong audit trails often expose sensitive voter information, while privacy-preserving schemes can be difficult to independently verify. These weaknesses erode public trust, increase the cost and complexity of conducting elections, and limit the ability of election officials to scale secure, transparent processes across jurisdictions.

Blockchain and biometric technologies each address parts of this problem space. Distributed ledgers provide tamper-evident, append-only records that can strength post-election auditability and make unauthorized modifications detectable. Biometric authentication – particularly facial recognition augmented with anti-spoofing (liveness) checks – offers a way to reliably bind a voter's identity to a single credential, reducing impersonation and duplicate-voter risks. However, both approaches also introduce new concerns: blockchain can make data widely visible unless appropriate raise privacy and replay-attack risks if not combined with strong anti-spoofing and careful data handling.

II. BACKGROUND

Elections form the foundation of democratic societies, yet both paper-based and electronic systems face persistent challenges such as ballot tampering, impersonation, duplicate voting, and the trade-off between voter privacy and result verifiability. These weaknesses reduce public trust and complicate secure, large-scale election management.

Blockchain technology addresses some of these problems through decentralization, immutability, and transparent audit trails. Once recorded, votes cannot be altered without detection, and observers can independently verify tallies. However, blockchain also introduces limitations: preserving ballot secrecy on a public ledger is difficult, and transaction throughput can restrict scalability.

To ensure only legitimate voters participate, biometric authentication-particularly facial recognition – offers a reliable identity check. Yet, facial recognition alone is vulnerable to spoofing through photos, videos, or deepfakes. Anti-spoofing techniques such as liveness detection and challenge – response mechanisms are therefore critical to prevent impersonation attacks.

Privacy in blockchain voting is further strengthened by zero-knowledge proofs (ZKPs). These allow voters to prove ballot validity and eligibility without revealing their identity or choice, while enabling auditors to verify tally correctness. ZKPs thus reconcile the tension between anonymity and verifiability, but require efficient implementation to remain practical.

Finally, successful adoption demands compatibility with legacy election infrastructure. Many proposals fail because they require complete replacement of voter registries and counting systems. A practical solution must integrate seamlessly, adding cryptographic guarantees and biometric safeguards without disrupting established legal and logistical processes.

III. PROBLEM STATEMENT

A key gap in existing work is practical interoperability with current election infrastructure. Many proposed advanced e-voting systems require wholesale replacement of voter registries, polling workflows, or ballot counting processes – an impractical barrier for election administrators who must preserve legal, logistical, and accessibility requirements. Moreover, few systems simultaneously achieve (1) tamper-resistant audit trails, (2) strong anti-spoof biometric authentication, and (3) cryptographic privacy that allows independent verification without exposing individual votes.

This paper aims to bridge that gap by presenting a secure privacy-preserving e-voting architecture that integrates blockchain immutability, anti-spoofing facial authentication, and zero-knowledge proofs to design emphasizes backward compatibility with existing voter databases and ballot counting systems, minimizing operational disruption while adding cryptographic guarantees disruptions safeguards. Our main contributions are: (a) a hybrid protocol that records minimal, no-identifying metadata on a distributed ledger to support audits; (b) an authentication pipeline using anti-spoofing facial recognition tied to ephemeral credentials; and (c) a ZKP based verification mechanism that proves correct tallying without revealing individual choices. We also evaluate practical deployment considerations – privacy regulations compliance, scalability, accessibility, and showing how the system can be adopted incrementally by election authorities.

IV. LITERATURE REVIEW

A. Blockchain Based E-Voting Systems

Blockchain based e-voting promises decentralization, transparency, and immutable auditability. For example, pilot systems in Estonia and Switzerland show how a distributed ledger can securely record and verify votes while improving transparency. In theory, blockchain (with smart contracts) can eliminate centralized authorities and tamper able records. In practice, studies note important benefits such as end-to-end verifiability, non-repudiation of ballots, and reduced trust assumptions in election officials.

- Benefits: Decentralization and immutable records reduce single points of failure and enhance audit trails. Transparency of a public ledger can increase voter trust. Systems leveraging smart contracts can automate vote tallying and result publication
- Limitations: However, blockchain e-voting suffers known drawbacks. The most-cited issues are voter privacy and performance. Many analysts point out that preserving ballot secrecy on a public chain is difficult, and high transaction latency limits scalability. Voters still need secure remote authentication and devices to connect, which introduces new attack surfaces. For example, Taş and Tanrıöver (2020) find that “privacy protection and transaction speed are most frequently emphasized problems in blockchain applications,” and they urge improving scalability and security for remote voting. Olaniyi et al. (2024) similarly note that blockchain voting faces cybersecurity risks, resource intensity, and infrastructure requirements that must be solved for real elections.
- Adoption Challenges: Deployment of blockchain voting also confronts institutional and technical hurdles. Legacy election authorities may lack expertise or legal frameworks for distributed ledgers. Moreover, blockchain systems must interoperate with existing election infrastructure. As Subramaniam et al. (2025) observe, “legacy systems are widely used … which may not support integration with blockchain technology”[5]. Reliable Internet access, voter education, and trust-building are additional societal barriers. In short, while blockchain can address many flaws of paper or centralized e-voting, it introduces new issues (e.g. privacy, throughput) and requires careful integration with current election processes[5].

B. Facial Recognition and Anti-Spoofing

Facial recognition (FR) has become popular for biometric authentication due to its convenience and non-contact nature. Modern FR systems achieve very high accuracy under ideal conditions. However, FR is vulnerable to spoofing: attackers can use printed photos, video replays, 3D masks, or even deepfake videos to impersonate voters. For this reason, any FR-based authentication must incorporate liveness detection or presentation-attack detection (PAD). PAD algorithms aim to distinguish a live human face from artifacts by analyzing cues such as texture, motion, depth, or interactive responses.

- Techniques: Approaches range from hardware-based (e.g. infrared sensors, 3D cameras, or light reflections) to software-based (e.g. texture analysis, blink or eye movement detection, machine-learning on video frames). With the advent of large deep-learning datasets, many state-of-the-art systems use convolutional networks to spot micro-textures or temporal inconsistencies that indicate a spoof. In practice, systems may combine multiple methods (multi-factor or multi-modal) to improve robustness.
- Current Performance: Reviews report that deep learning FAS now “dominates the field” with remarkable performance on benchmark datasets. Academic surveys highlight many novel solutions: e.g. combining color and depth, analyzing pulse (blood flow under skin), or challenging users (instructing them to turn head, smile, etc.). The U.S. voting system guidelines even anticipate biometric ID for polling places, emphasizing that alternative methods must exist when biometrics fail.
- Challenges and Weakness: Despite progress, anti-spoofing remains an open problem. Major surveys stress that existing PAD systems often lack generalization to new attacks and need more diverse data. For example, Sharma and Selwal (2023) note “limited generalization to unknown attacks” and “inadequacy of face datasets for [deep] models”. Novel attack types (e.g. high-fidelity masks or AI-generated videos) can defeat simple detectors, and “multi modal” approaches (combining vision with voice, fingerprint, etc.) are still rare. In practice, any face recognition system must also guard user privacy and bias; guidelines require fallback options (such as polling officials verifying identity if the camera fails or the face is unrecognizable). Overall, while deep networks have greatly improved liveness detection accuracy, the state-of-the-art methods remain sensitive to changing conditions and have notable gaps in practical robustness.

C. Zero Knowledge Proofs in Secure Voting

Zero-knowledge proofs are cryptographic tools that allow one party to prove knowledge of a secret (e.g. eligibility to vote or correct ballot form) without revealing the secret itself. In e-voting, ZKPs enable verifiable yet private operations. For example, a voter can prove that her encrypted ballot encodes exactly one valid choice without revealing which one. Similarly, election trustees can prove that they shuffled or decrypted ballots correctly without revealing intermediate results.

- Applications in Voting: Tanrıöver (2020) explain that proving a ballot is well formed (e.g. the vote lies within a valid range) is done via ZKPs so that “the encrypted data meets the properties of a valid ballot without compromising any information”. In mix-net or threshold-voting designs, ZKPs are required for “proof of correct shuffling” and “proof of correct decryption,” ensuring universal verifiability without leaking vote content. On the voter side, identity or credential verification can leverage ZKPs so a voter proves membership in the eligible set ZKPs so a voter proves membership in the eligible set without disclosing her identity. For instance, Miao (2023) describes a prototype where voters use ZKPs (combined with homomorphic encryption) to prove eligibility and ballot validity while keeping choices secret: “voters are eligible to vote without disclosing their identity and their vote is valid without revealing their choice”.
- Integration with Blockchain and Other Cryptography: or homomorphic tallying. Olaniyi et al. (2024) note that end-to-end verifiability can be achieved by using “advanced cryptographic techniques, such as homomorphic encryption and zero-knowledge proofs… in conjunction with blockchain”. In practice, such designs allow anyone to audit the election ledger and proofs, gaining confidence in the integrity of the count. For example, a voter’s device might publish an encrypted vote on a ledger and a ZKP of its form, and after the election, all tallies and ZK proofs can be checked publicly.
- Strengths and Weaknesses: The key strength of ZKPs is privacy preservation: they certify correctness without revealing sensitive data. They have become more practical with efficient proof systems (SNARKs, bulletproofs, etc.) and are standard in high-security settings. However, they also increase complexity. Many systems now incorporate ZKPs to ensure auditability and voter trust, but careful design is needed to avoid performance bottlenecks and usability issues.

V. PROPOSED SYSTEM

This proposed system leverages a hybrid cryptographic – biometric approach for secure, privacy – preserving, and verifiable e-voting. Its design emphasizes backward compatibility with existing election infrastructure while incorporating modern defenses against identity spoofing and vote tampering.

1. Client Application (Web/Mobile):

- Runs on voter devices and provides the primary interface for authentication and vote tampering.
- Implements liveness detection (texture analysis, blink detection, motion cues, challenge-response) using CNN based deep models.
- Generates ephemeral cryptographic keys bound to each voting session.
- Encrypts the ballot using homomorphic encryption and attaches Zero-Knowledge Proof proving that the vote is valid and originates from an eligible voter without revealing identity or choice.

2. Authentication Service:

- Validates liveness and identity by comparing biometric signatures with voter registry data.
- Issues anonymous credentials (unlikeable tokens) to ensure that once authenticated, the voter’s ballot cannot be linked back to their identity.

- Uses FIDO2/ WebAuthn to prevent phishing, replay attacks, and credential theft.

3. Middleware/ API Gateway:

- Serves as the central validation layer between the client, blockchain, and existing election infrastructure.
- Verifies ZKPs and prevents malformed or duplicate ballots.
- Provides interoperability adapters for existing voter databases and ballot counting systems, ensuring minimal disruption.

4. Permissioned Blockchain Layer:

- Maintain a distributed, immutable ledger of encrypted ballots and ZKPs.
- Anchors hashes of transactions to a public blockchain (e.g., Ethereum, Bitcoin) for tamper-proof guarantees.
- Provides transparency by allowing auditors to independently verify ballots and proofs without accessing sensitive data.

5. Tallying & Trustees:

- Ballots are shuffled and decrypted using verifiable mix-nets or threshold decryption.
- Trustees provide cryptographic proofs that decryption and tallying were performed correctly.
- Results are published both on-chain (as encrypted/verifiable proofs) and off-chain (for traditional audit purposes).

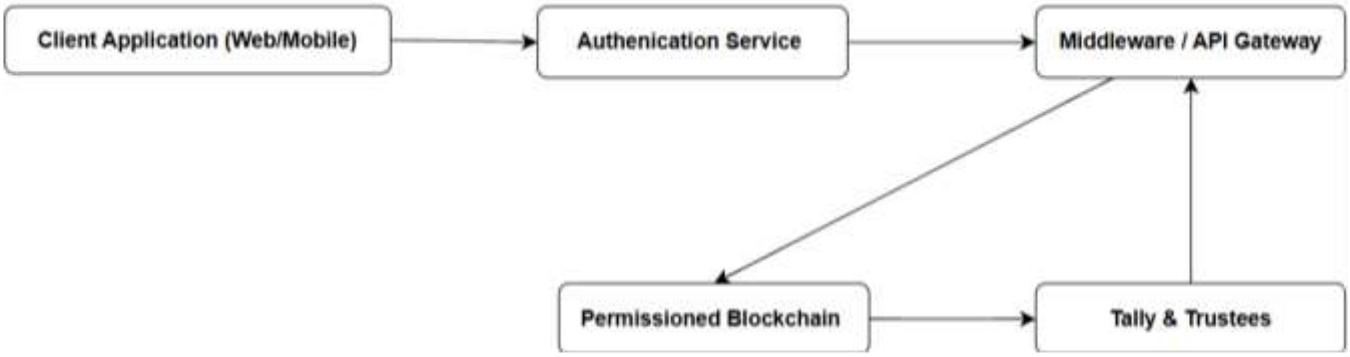


Fig. 1: Proposed system architecture

VI. METHDOLOGY

1. Voter Authentication & Anti-Spoofing:

- Each voter undergoes facial recognition with multi-modal liveness checks (blink detection, texture analysis, depth cues).
- Resistant to photo, video, deepfake, and 3D mask attacks through CNN-based classifiers trained on benchmark datasets like CASIA-FASD, Replay-Attack, and OULU-NPU.
- Backup authentication (manual verification, OTP-based) ensures accessibility for voters who cannot pass biometric checks.

2. Vote Casting with ZKPs:

- Once authenticated, the system issues a one-time anonymous credential.
- Voters encrypt their ballot with homomorphic encryption and attach a ZKP ensuring the vote is valid (exactly one candidate selected, no tampering).
- ZKPs also prevent double voting, since each anonymous credential is valid for only one submission.

3. Blockchain Integration:

- Encrypted ballots and proofs are posted to the permissioned blockchain.
- The blockchain ensures immutability, non-repudiation, and public verifiability.
- Anchored hashes on a public chain guarantee that even consortium administrators cannot alter results undetected.

4. Tallying & Verification:

- Trustees collaboratively decrypt ballots using threshold cryptography.
- ZKPs and mix-nets ensure that votes are shuffled before decryption, breaking any link between voters and ballots.
- Independent auditors can verify the integrity of the tally by checking published ZKPs and blockchain records.

5. Threat Mitigation & Strategy:

- Impersonation attacks mitigated with anti-spoof + WebAuthn.
- Vote tampering mitigated by immutable blockchain records + ZKPs.
- Privacy leakage prevented with anonymous credentials and unlikeable ballots.
- Coercion attacks countered with re-voting and receipt-free ballots.
- Double voting prevented through one-time credential issuance.

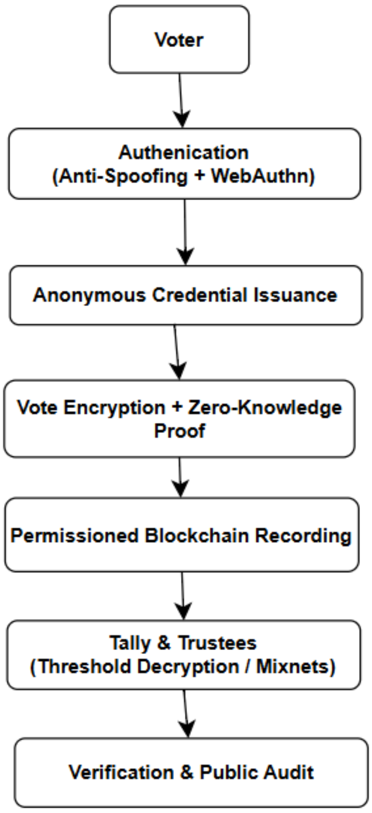

Voter
Authenication (Anti-Spoofing + WebAuthn)
Anonymous Credential Issuance
Vote Encryption + Zero-Knowledge Proof
Permissioned Blockchain Recording
Tally & Trustees (Threshold Decryption / Mixnets)
Verification & Public Audit

Fig 2: Blockchain based secure e-voting workflow

VII. EXPECTED OUTCOMES

The expected outcomes of the proposed system span technical, operational, and societal dimensions:

1. Enhanced Security:

- Reduction of impersonation risks through muti-modal facial anti-spoofing with ≥95% accuracy.
- Resistance to phishing and credential replay via FIDO2/WebAuthn authentication.
- Blockchain backed immutability ensures votes cannot be altered or deleted once recorded.

2. Strong Privacy Guarantees:

- Voter identity remains unlikable to ballots due to anonymous credential issuance.

- Zero Knowledge Proofs enable verifiability without leaking vote content.
- Coercion resistance is achieved via receipt-free protocols and re-voting options.

3. Operational Efficiency:

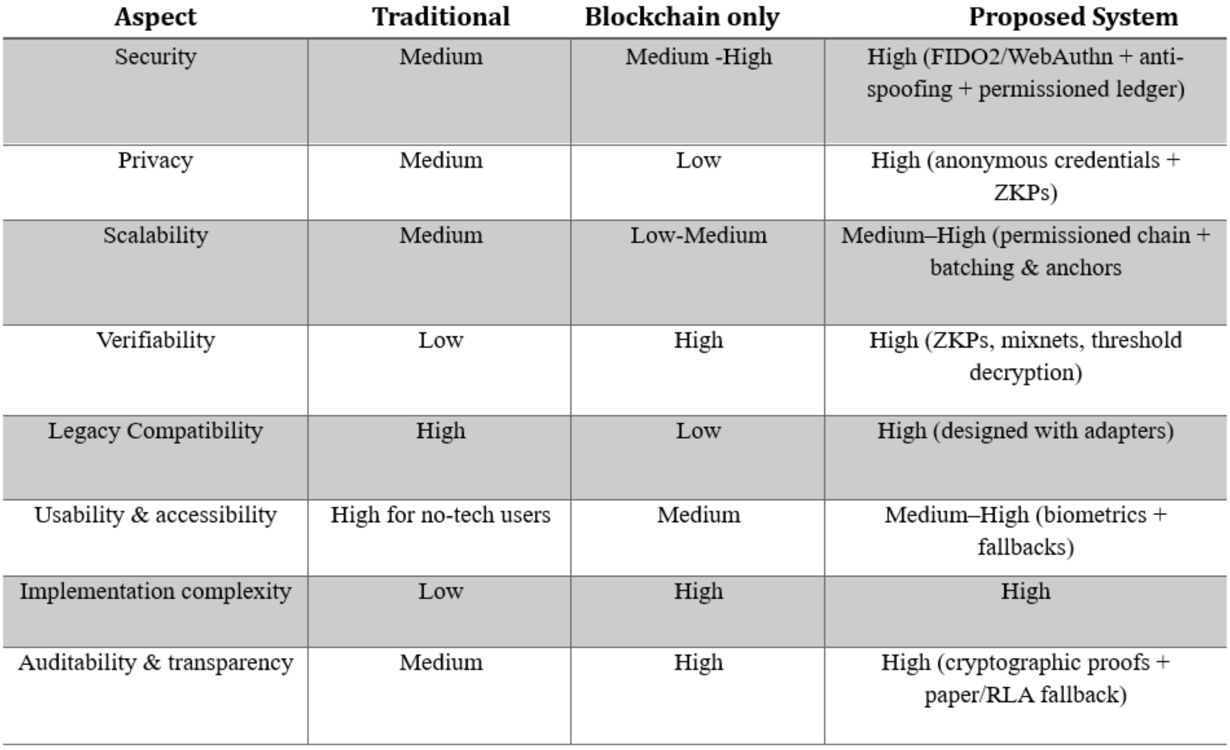
- Ballot casting and verification designed to complete in under 5 seconds per voter.
- Election tallying and verification expected to finish within a few hours of poll closure, even in large-scale elections.
- Hybrid deployment ensures compatibility with paper trails and Risk-Limiting Audits (RLAs).

4. Transparency and Trust:

- Auditors, observers, and the public can independently verify the correctness of election results using blockchain records and ZKPs.
- Ensures tamper-evident auditability with mathematically verifiable cryptographic guarantees.
- Increased voter confidence due to transparency and privacy-preserving guarantees.

5. Scalability & Real-World Deployment Feasibility:

- The system is scalable for national-level elections with millions of voters.
- Designed to integrate into existing voter registries and ballot counting systems, reducing barriers to adoption.
- Future-proof with planned upgrades to post-quantum cryptography and multi-device authentication.



Aspect	Traditional	Blockchain only	Proposed System
Security	Medium	Medium -High	High (FIDO2/WebAuthn + anti-spoofing + permissioned ledger)
Privacy	Medium	Low	High (anonymous credentials + ZKPs)
Scalability	Medium	Low-Medium	Medium–High (permissioned chain + batching & anchors
Verifiability	Low	High	High (ZKPs, mixnets, threshold decryption)
Legacy Compatibility	High	Low	High (designed with adapters)
Usability & accessibility	High for no-tech users	Medium	Medium–High (biometrics + fallbacks)
Implementation complexity	Low	High	High
Auditability & transparency	Medium	High	High (cryptographic proofs + paper/RLA fallback)

Table1: Comparative analysis of expected outcomes across Traditional, Blockchain-only, and Proposed E-Voting systems

VIII. CONCLUSION

The proposed system integrates phishing – resistant authentication (FIDO2/WebAuthm), client-side, liveness checks, and end-to-end verifiable ballot handling (via mix nets or homomorphic tallying with threshold decryption). These are supported by a paper trail and Risk – Limiting Audits (RLAs) to ensure integrity, privacy, and operational compliance. Together, these measures significantly raise the barrier against attacks while providing transparent, auditable elections outcomes.

IX. FUTURE WORK

Future work will focus on building a full-stack prototype with open-source release, followed by large-scale performance and scalability testing to ensure suitability for national elections. Further research is needed to improve the efficiency of zero-knowledge proofs and enhance the robustness of anti-spoofing techniques against emerging threats such as deepfakes and 3D masks. Usability and accessibility studies will ensure the system is inclusive for diverse populations, while legal and regulatory compliance analysis will guide real-world deployment. Red-team evaluations and independent cryptographic audits will strengthen trust and resilience. Additional directions include exploring post-quantum secure cryptography, developing hybrid deployment models for gradual adoption, and establishing transparent governance and audit frameworks. Together, these efforts will help transition the proposed design from conceptual architecture to a deployable, verifiable, and future-ready e-voting system.

X. REFERENCES

[1] Atik, M.A.K., Tarin, S. and Rahman, M. (2025) ‘A comprehensive analysis of blockchain-based voting systems: enhancing transparency and security’, in *Proceedings of the 3rd International Conference on Computing Advancements (ICCA 2024)*, Dhaka, Bangladesh, June 2025. ACM, pp. XXX–XXX. doi:10.1145/3723178.3723275.

[2] Berenjestanaki, M.H., Barzegar, H.R., El Ioini, N. and Pahl, C. (2024) ‘Blockchain-Based E-Voting Systems: A Technology Review’, *Electronics*, 13(1), 17. MDPI. doi:10.3390/electronics13010017.

[3] Cong, L.T.Q., Thuy, N.D.P., Nhi, H.T.N. and Anh, T.V. (2024) ‘Blockchain-Based Electronic Voting: Lessons from Estonia’, *Vietnamese Journal of Legal Sciences*, 11(2), pp.27–39. Sciendo. doi:10.2478/vjls-2024-0009.

[4] Huber, N., Küsters, R., Liedtke, J. and Rausch, D. (2024) ‘ZK-SNARKs for Ballot Validity: A Feasibility Study’, in *Lecture Notes in Computer Science*, vol. 15014, pp.107–123. Springer. doi:10.1007/978-3-031-72244-8_7.

[5] Jafar, U., Aziz, M.J.A. and Shukur, Z. (2021) ‘Blockchain for Electronic Voting System—Review and Open Research Challenges’, *Sensors*, 21(17), 5874. MDPI. doi:10.3390/s21175874.

[6] Joni, S.A., Rahat, R., Tasnin, N., Ghose, P., Uddin, M.A. and Ayoade, J. (2024) ‘Hybrid-Blockchain-Based Electronic Voting Machine System Embedded with Deepface, Sharding, and Post-Quantum Techniques’, *Blockchains*, 2(4), pp.366–423. MDPI. doi:10.3390/blockchains2040017.

[7] Miao, Y. (2023) ‘Secure and Privacy-Preserving Voting System Using Zero-Knowledge Proofs’, *Applied and Computational Engineering*, 8(1), pp.328–333. doi:10.54254/2755-2721/8/20230181.

[8] Ohize, H.O., Onumanyi, A.J., Umar, B.U. et al. (2025) ‘Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges’, *Cluster Computing*, 28, Article 132. Springer. doi:10.1007/s10586-024-04709-8.

[9] Sharma, D. and Selwal, A. (2023) ‘A survey on face presentation attack detection mechanisms: hitherto and future perspectives’, *Multimedia Systems*, 29(3), pp.1527–1577. Springer. doi:10.1007/s00530-023-01070-5.

[10] Subramaniam, N. et al. (2025) ‘Blockchain-based voting systems enhancing transparency and security in electoral processes’, *ITM Web of Conferences*, 76, 02004. EDP Sciences. doi:10.1051/itmconf/20257602004.

[11] Taş, S. and Tanrıöver, Ö.Ö. (2020) ‘A systematic review of challenges and opportunities of blockchain for e-voting’, *Symmetry*, 12(8), 1328. MDPI. doi:10.3390/sym12081328.

[12] Xing, H., Tan, S.Y., Qamar, F. and Jiao, Y. (2025) ‘Face Anti-Spoofing Based on Deep Learning: A Comprehensive Survey’, *Applied Sciences*, 15(12), 6891. MDPI. doi:10.3390/app15126891.