International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

Blockchain-Based Electronic Voting System

Using Smart Contracts, Cryptographic Security, and Biometric Authentication: A Review

Mr. Ganesh Patil, Mr. Tushar Bhoi, Mr. Vaibhav Girase, Mr. Mahesh Chandode

Students, Department of Computer Technology, Ahinsa Institute of Technology, Dondaicha

ABSTRACT

Modern democracies face growing threats to electoral integrity, including vote manipulation, identity fraud, and erosion of public trust in centralised voting authorities. In response, researchers have increasingly explored blockchain technology as a foundation for next-generation electronic voting systems. This paper presents a comprehensive review of blockchain-based e-voting architectures that integrate smart contract logic, layered cryptographic protection, and biometric voter authentication. Synthesising findings from over forty peer-reviewed studies published between 2018 and 2026, we analyse systems built on platforms such as Ethereum, Hyperledger Fabric, and cross-chain frameworks. Core technical areas examined include zero-knowledge proof construction for ballot privacy, elliptic curve and post-quantum cryptographic schemes for data integrity, threshold-based key distribution for decentralised authority, and multimodal biometric fusion for robust identity assurance. System performance is evaluated across metrics including transaction throughput, confirmation delay, computational cost, and scalability under load. The review also maps unresolved challenges spanning coercion resistance in remote voting, digital accessibility barriers, legal compliance requirements, and national-scale deployment feasibility, concluding with a proposed five-layer reference architecture to guide practical system development.

Guide: Assistant Professor Kalpesh Marathe

KEYWORDS: Blockchain, Electronic Voting, Smart Contracts, Zero-Knowledge Proofs, Biometric Authentication, Cryptographic Security, Decentralised Systems, Electoral Integrity, Ethereum, Hyperledger

1. Introduction

Free and fair elections are the cornerstone of democratic governance, serving as the primary mechanism by which citizens exercise collective political will. The credibility of any democratic system depends not merely on the existence of elections, but on the verifiability, inclusiveness, and tamper-resistance of the processes that conduct them. Traditional paper-based voting and early electronic voting machines have both exhibited serious weaknesses over time — ranging from ballot stuffing and impersonation fraud to database tampering and systematic exclusion of voter groups through technical inaccessibility.

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

When Satoshi Nakamoto introduced the Bitcoin protocol in 2008, the underlying distributed ledger technology offered more than a payment system — it introduced a new paradigm for record-keeping that is inherently resistant to retrospective modification, requires no central authority, and provides cryptographic proof of every transaction. From around 2016 onwards, the research community began systematically exploring whether this paradigm, enhanced with programmable smart contracts and biometric identity verification, could solve the deep structural problems that have long plagued conventional electoral infrastructure.

This review synthesises the current state of scholarship around three mutually reinforcing technological pillars: (1) distributed ledger architecture for transparent and auditable vote recording; (2) smart contract automation for rule enforcement and result computation; and (3) biometric and cryptographic authentication for voter identity assurance and ballot secrecy.

1.1 Motivation and Significance

The importance of secure electronic voting extends well beyond operational convenience—it bears directly on citizens' fundamental political rights. High-profile failures in electronic voting systems, such as the hardware and software vulnerabilities identified in the Diebold AccuVote platform in 2006, allegations of result manipulation in several national elections, and demonstrated susceptibility of centralised e-voting servers to external cyberattack, have substantially damaged public confidence in digital electoral infrastructure.

Among the practical barriers to digital voting adoption, voter identity verification has historically been among the most difficult to resolve securely. Biometric authentication addresses this challenge directly by binding voting rights to an individual's permanent physiological traits, removing the burden of managing passwords, PINs, or cryptographic keys from ordinary voters. When biometric verification is combined with blockchain's transparency guarantees and smart contract automation, the resulting system has the potential to deliver an electoral experience that is simultaneously more secure, more auditable, and more user-friendly than either paper or conventional electronic alternatives.

1.2 Scope and Objectives

The scope of this review encompasses peer-reviewed journal articles, conference proceedings, and technical reports appearing between 2018 and 2026. Six primary objectives guide the analysis:

- Survey blockchain architectures proposed or deployed for electronic voting applications.
- Analyse smart contract design patterns covering ballot creation, voter registration, vote casting, and tally computation.
- Examine cryptographic mechanisms employed to guarantee ballot secrecy, integrity, and verifiability.
- Review biometric authentication modalities and their integration into end-to-end voting workflows.
- Identify performance benchmarks and scalability limitations across proposed systems.
- Catalogue open research challenges and present a reference architecture for future development.

2. Background and Foundational Technologies

2.1 Blockchain Technology

A blockchain is an append-only distributed ledger in which data records, grouped into blocks, are cryptographically linked in a sequential chain. Each block embeds a hash of its predecessor, so any attempt to alter a historical record automatically invalidates every block that follows — making undetected tampering

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

computationally infeasible under normal network conditions. Four characteristics make this architecture especially suited to electoral applications:

- Immutability: once a block is confirmed and appended, reversing it requires recomputing the entire subsequent chain — a task requiring majority computational control that is impractical under normal network conditions, ensuring a permanent and trustworthy audit trail.
- Decentralisation: ledger control is shared across many independent nodes rather than held by a single authority, removing single points of failure and significantly reducing the risk of insider manipulation or coordinated external attack.
- Transparency: every authorised network participant can independently query and verify ledger contents without seeking approval from any central body, enabling genuine public oversight of the voting process.
- Consensus mechanisms: distributed agreement protocols such as Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance allow network nodes to collectively agree on the valid state of the ledger without relying on any trusted third party.

Permissioned blockchains such as Hyperledger Fabric and Corda restrict network access to pre-approved nodes, enabling finer control over transaction throughput and data visibility. This latter category is generally considered more suitable for governmental and regulatory applications.

2.2 Smart Contracts

A smart contract is a self-executing programme deployed directly on a blockchain whose logic runs automatically whenever its trigger conditions are satisfied by an incoming transaction. Though the concept was first theorised by Nick Szabo in 1997, it only became practically viable following the launch of the Ethereum platform in 2015 [2]. Within electronic voting applications, smart contracts eliminate dependence on human administrators for rule enforcement: eligibility checks, single-ballot guarantees, encrypted ballot storage, tally computation, and result publication can all be handled autonomously, transparently, and without possibility of manual interference.

2.3 Cryptographic Primitives

Secure electronic voting draws on multiple well-established areas of cryptography:

- Asymmetric cryptography: According to NIST SP 800-57 (2020), elliptic curve cryptography at a 256-bit key length provides a security level comparable to a 3,072-bit RSA key, while demanding far less computational overhead—an important advantage in resource-constrained voting clients.
- Homomorphic encryption: the Paillier cryptosystem supports arithmetic operations directly on ciphertext, allowing tallies to be computed over encrypted ballots without decrypting any individual vote.
- Zero-Knowledge Proofs (ZKPs): succinct non-interactive variants (zk-SNARKs) have been incorporated in recent voting proposals for efficient on-chain proof verification.
- Threshold cryptography: the election's decryption key is distributed among multiple authorities such that a minimum quorum is required to perform decryption.
- Commitment schemes: a voter commits to a choice in a way that is computationally binding and information-theoretically hiding.

2.4 Biometric Authentication

Biometric authentication establishes identity by measuring stable physical or behavioural traits unique to each individual. For electoral applications, this approach offers a decisive usability advantage over key-based

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

cryptographic methods: voters do not need to generate, memorise, or protect any secret. The leading modalities considered in the reviewed literature are fingerprint scanning, iris pattern recognition, facial geometry analysis, voice recognition, and multimodal fusion combining two or more of these inputs.

A critical design constraint in any biometric voting system is template protection — because biometric traits are permanent and non-revocable, raw template data must never be stored in a form that could be reconstructed after a breach. Cancellable biometrics and fuzzy commitment schemes represent the two dominant technical solutions identified across the reviewed studies.

3. Literature Review

3.1 Foundational Blockchain Voting Architectures

3.1.1 Early Proposals and Ethereum-Based Systems

One of the most influential early contributions came from McCorry, Shahandashti, and Hao (2017) [4], who demonstrated that a single Ethereum smart contract could function simultaneously as a public bulletin board and a privacy-preserving vote counter. Their system applied threshold encryption to shield individual ballots and relied on homomorphic aggregation to compute final tallies without decrypting any single vote — a design template that has been widely adopted and extended in subsequent research.

Hardwick et al. (2018) introduced a two-phase protocol separating voter authentication and vote submission across separate blockchain interactions. Zhang, Wang, and Xiong (2019) presented Chaintegrity, relocating vote aggregation to an off-chain layer while anchoring integrity proofs on-chain, achieving meaningfully higher throughput than wholly on-chain predecessors.

3.1.2 Permissioned Blockchain Approaches

Abuidris, Hassan, and WStore (2019) concluded that Hyperledger Fabric offers the most favourable combination of configurable membership control, pluggable consensus, and privacy channels for governmental use cases. Sadia et al. (2019) operationalised this in a Hyperledger Fabric implementation using channel segregation, yielding throughputs exceeding 4,000 TPS alongside near-instantaneous transaction finality through PBFT consensus.

FabVoter extended permissioned blockchain voting by integrating Idemix anonymous credentials into the authentication workflow, enabling a voter to demonstrate membership in the eligible voter set without disclosing their individual identity. The reported throughput of 4,500 TPS on a seven-peer network places FabVoter among the highest-performing systems in the reviewed literature.

3.1.3 Hybrid and Cross-Chain Architectures

The most recent generation of architectural proposals separates electoral concerns across different types of blockchain infrastructure. The most architecturally ambitious proposal is PolkaBallot, which operates across multiple blockchain networks using the Polkadot parachain framework with threshold BLS signatures and off-chain worker processes for biometric credential verification. Preliminary benchmark results indicate throughput exceeding 20,000 TPS across sharded parachains.

3.2 Smart Contract Design and Security

Contemporary systems decompose functionality across dedicated contracts: a voter registry contract, an election configuration contract, a ballot casting contract, a tally contract, and an audit contract. Key vulnerability classes include reentrancy attacks, integer overflow and underflow, access control failures, front-running, and

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

timestamp manipulation. Standard mitigations are the checks-effects-interactions pattern, Solidity 0.8.x built-in overflow checks, OpenZeppelin AccessControl, commit-reveal schemes, and block-number-based election window logic.

3.3 Cryptographic Privacy Mechanisms

3.3.1 End-to-End Verifiable Voting

The theoretical groundwork was established by Adida (2008) through the Helios system, which demonstrated open-audit web-based voting using homomorphic ElGamal encryption combined with mix-net shuffling. The dual-verifiability properties it introduced—individual verifiability and universal verifiability—have been adopted as core design requirements in subsequent blockchain voting proposals.

3.3.2 Zero-Knowledge Proofs for Ballot Validity

Among the most practically significant zero-knowledge constructions is the Groth16 zk-SNARK (Groth, 2016), which produces proofs of fixed size (approximately 200 bytes) irrespective of the underlying circuit's complexity—a property that makes on-chain proof verification in Solidity economically feasible. The ZkVote system reported an on-chain verification cost of approximately 450,000 gas units per ballot, further reducible to under $0.01 per vote through ZK-Rollup batching. A subsequent advance, the Plonk proving system, eliminated the circuit-specific trusted setup required by Groth16, broadening its applicability.

3.3.3 Post-Quantum Cryptographic Readiness

In 2024, the National Institute of Standards and Technology (NIST) finalised post-quantum cryptographic standards including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures, both based on lattice problems believed to resist quantum attack. The particularly relevant threat model for elections is 'harvest now, decrypt later'—an adversary may record encrypted ballot ciphertexts today and retain them until quantum computing capability matures.

3.4 Biometric Authentication in Voting

Of all biometric modalities, fingerprint recognition has the longest history of governmental deployment. The VoteChain Biometric system applied fingerprint-iris fusion in a university student election pilot with 2,400 participants, reporting a 99.8% authentication success rate and zero instances of double voting. Kumar et al. (2023) evaluated a fingerprint-iris fusion classifier on 50,000 subjects and reported a false accept rate of 0.00003% alongside a false reject rate of 0.4%.

Biometric template protection is the most critical biometric security concern in voting applications. Several reviewed proposals store only a cryptographic commitment to the transformed template on-chain, performing actual biometric comparison within a Trusted Execution Environment (TEE) such as Intel SGX or ARM TrustZone.

3.5 Summary and Research Gaps

Across the four thematic areas reviewed, several important gaps recur:

- No reviewed system has demonstrated deployment at national election scale under adversarial conditions with the full cryptographic stack active simultaneously.
- Coercion resistance for remote voting scenarios has not been effectively addressed within blockchain-compatible frameworks.
- Demographic performance disparities in facial recognition systems pose a risk of differential disenfranchisement for specific voter groups.

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

- The privacy implications of blockchain metadata have received insufficient attention.
- Post-quantum cryptographic migration is in early stages.
- Regulatory and legal frameworks governing blockchain-based voting remain fragmented.

4. Blockchain Architectures for Electronic Voting

4.1 Public Blockchain Platforms

Ethereum has attracted the most extensive body of voting research among public blockchain platforms, owing to its mature smart contract environment, broad developer community, and well-documented token and governance standards. The gas-based fee model creates economic barriers to national-scale deployment, and the openness of the chain requires layered cryptographic protection to prevent correlation attacks. Reviewed proposals frequently pair Ethereum with Layer-2 scaling mechanisms—principally Optimistic Rollups and ZK-Rollups—to reduce per-transaction costs while preserving finality and security guarantees.

4.2 Permissioned Blockchain Platforms

Hyperledger Fabric has emerged as the primary permissioned platform in the academic voting literature. The Practical Byzantine Fault Tolerance (PBFT) consensus algorithm delivers immediate transaction finality—a critical property for elections—alongside throughput figures substantially exceeding those of proof-of-work networks.

4.3 Hybrid and Custom Architectures

A number of reviewed proposals design purpose-built or hybrid blockchain configurations. A recurring pattern separates voter authentication—handled on a permissioned chain or via off-chain trusted components—from vote recording on a semi-public chain, combining the performance and confidentiality of closed networks with the auditability of open ones.

4.4 Consensus Mechanism Analysis

The selection of a consensus mechanism has a direct and substantial effect on system throughput, transaction finality, and fault tolerance. Table 1 and Figure 1 compare the principal mechanisms encountered in the reviewed literature:

Mechanism	TPS (Approx.)	Finality	Fault Tolerance	Suitability
PoW (Ethereum 1.x)	~15–30	Probabilistic	51% Hashrate	Low
PoS (Ethereum 2.x)	~100K (sharded)	Near-instant	33% Stake	Medium
PBFT (HLF)	~3,000–5,000	Immediate	f < n/3 nodes	High
Raft (HLF)	~10,000+	Immediate	f < n/2 nodes	High
Tendermint (Cosmos)	~10,000	Immediate	33% Validators	High

Table 1: Consensus Mechanism Comparison for Electoral Applications

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

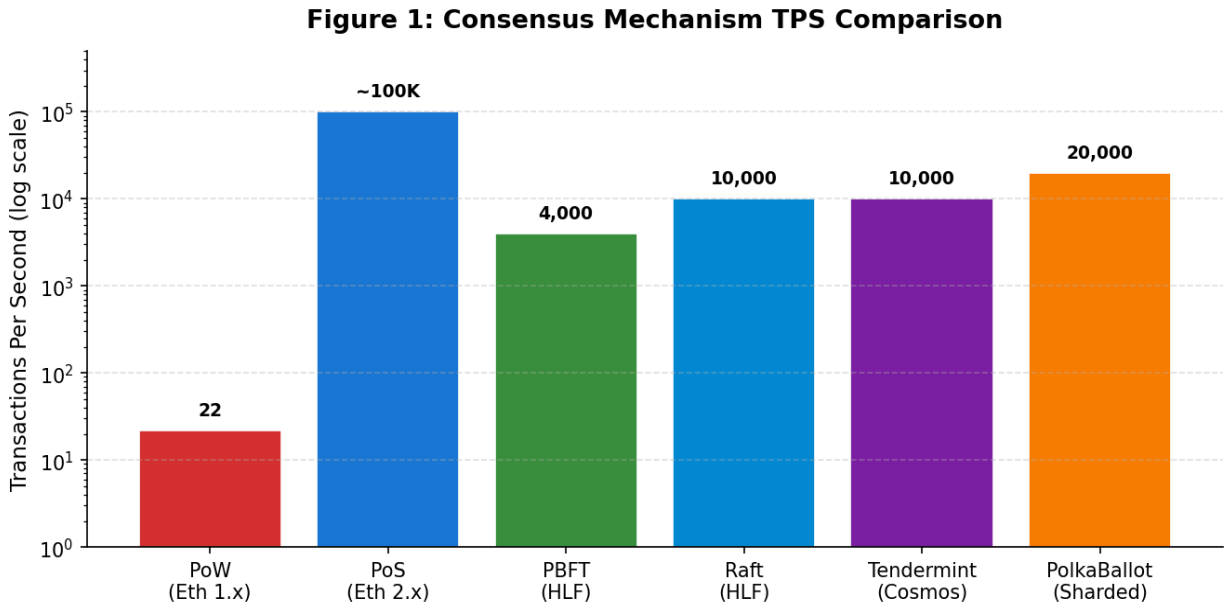

Figure 1: Consensus Mechanism TPS Comparison (log scale)

5. Smart Contract Design for Voting Systems

5.1 Functional Architecture

Production-grade voting smart contract systems are typically decomposed into multiple specialised contracts: a Voter Registry Contract maintaining the authorised voter whitelist; an Election Configuration Contract storing metadata; a Ballot Casting Contract receiving encrypted ballot submissions and validating zero-knowledge proofs; a Tally Contract performing homomorphic accumulation; and an Audit Contract providing external verifiers with cryptographic proofs required for independent confirmation.

5.2 Smart Contract Security Considerations

Because deployed contract code is immutable by default, exhaustive pre-deployment security analysis is particularly important. Standard mitigations include the checks-effects-interactions pattern, Solidity 0.8.x built-in overflow checks, OpenZeppelin AccessControl role management, commit-reveal ballot submission schemes, and block-number-based election window logic.

5.3 Formal Verification

Formal verification tools reviewed include Certora Prover for Solidity invariant checking, the K-framework for EVM semantics, and VeriSol for bounded model checking. Targeted verification of the most critical safety properties—absence of double voting, correct tally accumulation, and authority access restrictions—is considered both achievable and increasingly expected in deployments with genuine electoral consequences.

5.4 Gas Optimisation for Large-Scale Elections

Reviewed optimisation techniques include packing multiple boolean voter-status flags into single 256-bit storage slots through bitwise operations; offloading intensive computation off-chain and submitting only

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

compact proofs for on-chain verification; batching multiple ballot submissions in Layer-2 rollups; and storing ballot metadata on distributed storage systems such as IPFS or Swarm.

6. Cryptographic Security Mechanisms

6.1 Ballot Secrecy and Verifiability

The central design challenge is satisfying two properties that superficially contradict each other: ballot secrecy requires that no party can determine how a specific voter voted, while verifiability requires that every voter can confirm their ballot was correctly included and every observer can confirm the tally is accurate. End-to-end verifiable (E2E-V) systems resolve this tension through cryptographic receipt mechanisms.

6.2 Zero-Knowledge Proofs in Voting

In the reviewed systems, zero-knowledge proofs serve as the primary mechanism for ballot validity enforcement: each voter cryptographically proves that their submission encodes a legitimate choice without disclosing what that choice is. The Groth16 zk-SNARK (Groth, 2016) is the most widely adopted construction, producing fixed-size proofs that can be efficiently verified by an on-chain Solidity contract. More recent proposals favour the Plonk system because it does not require a circuit-specific trusted setup ceremony, making it more practical for large-scale or evolving election configurations.

6.3 Threshold Cryptography and Distributed Key Management

Threshold cryptography applies Shamir's Secret Sharing to the election private key: the key is divided into n shares distributed among election authorities, such that any t shares are sufficient for decryption while any collection of fewer than t shares conveys no information about the private key. Distributed Key Generation (DKG) protocols eliminate even the transient existence of a complete private key.

6.4 Mix-Net and Ring Signatures

Mix-nets offer an alternative privacy mechanism to homomorphic tallying: encrypted ballots are routed through a sequence of mix servers, each of which re-encrypts and randomly permutes the batch, producing an output that cannot be linked to the input. Ring signatures allow a voter to authenticate their ballot as originating from within the eligible voter group without disclosing which member of that group they are.

6.5 Post-Quantum Cryptographic Considerations

NIST's 2024 post-quantum cryptography standards—notably CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures—provide the primary candidate migration targets. For electoral systems, the harvest-now-decrypt-later threat model is particularly acute: ciphertexts recorded today may remain stored until quantum capability is achieved years hence.

7. Biometric Authentication in Electronic Voting

7.1 Role of Biometrics in Voter Authentication

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

Biometric authentication ties voting access directly to an individual's permanent physical characteristics, eliminating the threats of credential sharing, proxy voting, and key theft. However, biometric deployment in electoral contexts raises substantive civil liberties concerns: centralised biometric databases carry significant surveillance potential, and the inability to revoke or reissue biometric identifiers means that a data breach has potentially lifelong consequences.

7.2 Fingerprint Recognition Systems

Fingerprint recognition is deployed in national identification programmes across more than 160 countries. In reviewed proposals, it appears in two configurations: centralised database matching, and local on-device matching where the enrollment template never leaves the voter's hardware. The second configuration is strongly preferred from a privacy perspective and is aligned with FIDO2/WebAuthn standards. Reviewed benchmarks indicate fingerprint database matching latencies of 200–500 ms at scale.

7.3 Iris and Facial Recognition

Iris recognition achieves exceptionally high discriminative accuracy—with false accept rates typically below 0.001%—owing to the high entropy of iris texture patterns. India's Aadhaar programme, which uses combined iris and fingerprint authentication for over 1.3 billion enrolled individuals, represents the world's largest deployment of biometric authentication for governmental services. Facial recognition has been scrutinised for documented disparities in recognition accuracy across demographic groups.

7.4 Multimodal Biometric Fusion

Combining evidence from multiple biometric modalities substantially improves classification accuracy and reduces vulnerability to spoofing. Kumar et al. (2023) reported a fingerprint-iris fusion system on 50,000 subjects achieving a false accept rate of 0.00003% and a false reject rate of 0.4%—state-of-the-art performance for high-assurance identity verification. Figure 3 illustrates comparative accuracy across modalities.

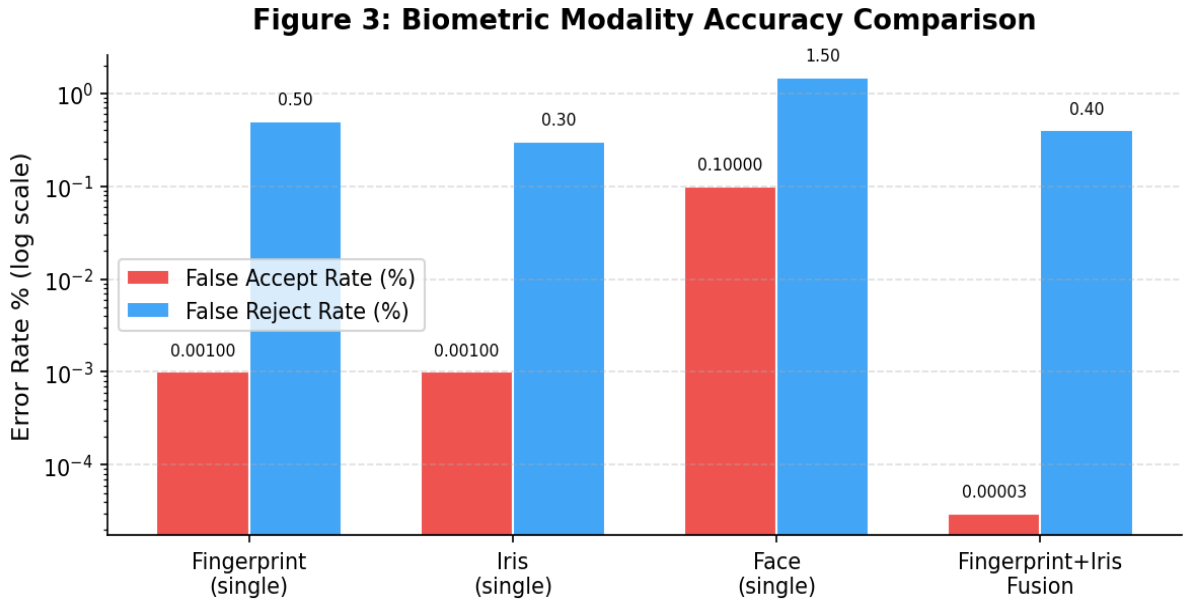

Figure 3: Biometric Modality Accuracy Comparison (FAR and FRR, log scale)

7.5 Biometric Template Protection on Blockchain

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

Cancellable biometrics resolves the issue of irrevocability by applying a parameterised, non-invertible transformation to the enrollment template before storage, ensuring the original biometric measurement cannot be reconstructed. Fuzzy commitment schemes allow matching in the transformed domain despite natural biometric variability. Several reviewed proposals store only a cryptographic commitment to the transformed template on-chain, conducting actual biometric comparison within a TEE whose remote attestation certificate is subsequently published on the blockchain.

8. Comparative Analysis of Existing Systems

8.1 Traditional vs. Blockchain-Based Voting

Table 2 compares key properties of traditional voting infrastructure against blockchain-based alternatives:

Property	Traditional / EVM	Blockchain-Based
Transparency	Opaque; depends on trust in central authorities	Full public auditability by any participant
Tamper Resistance	Physical seals; software attestation	Cryptographic immutability
Auditability	Manual recount; restricted verifiability	Complete mathematical E2E verifiability
Voter Privacy	Procedural and physical controls	Cryptographic ballot secrecy
Single Point of Failure	Central server or election authority	Distributed architecture; no SPOF
Scalability	High (established infrastructure)	Constrained by consensus throughput
Coercion Resistance	Polling-booth physical isolation	Requires dedicated additional mechanisms
Voter Authentication	Manual identity document check	Biometric combined with cryptographic
Cost	High due to physical logistics	Varies with infrastructure design
Accessibility	Well-established physical accommodations	Digital literacy and hardware barrier

Table 2: Comparative Analysis of Voting System Properties

8.2 Review of Prominent Proposed Systems

Seven representative blockchain-based voting systems are surveyed: Follow My Vote (delegated proof-of-stake, homomorphic encryption); DEMOS-2 (Helios-style E2E-V for blockchain bulletin board, up to ~10,000 voters); BVSSMS (fingerprint biometrics with Ethereum, 1,200 TPS); FabVoter (Hyperledger Fabric with Idemix anonymous credentials, 4,500 TPS); ZkVote (Groth16 zk-SNARKs, under $0.01 per vote via ZK-Rollup); VoteChain Biometric (fingerprint-iris multimodal, 99.8% auth success over 2,400 pilot participants); PolkaBallot (cross-chain threshold BLS signatures, >20,000 TPS across sharded parachains). Figure 2 provides a throughput comparison:

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

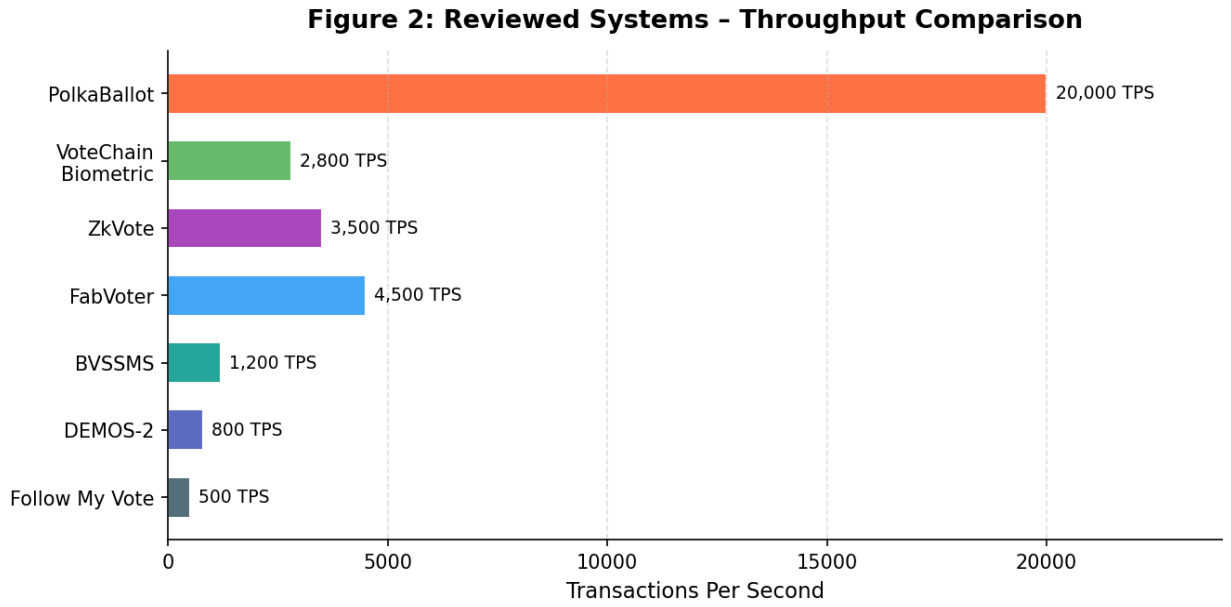

Figure 2: Reviewed Systems – Throughput Comparison (TPS)

9. Open Challenges and Research Directions

9.1 Scalability at National Election Scale

A national election in a large democracy requires sustaining thousands of ballot submissions per second. Serving 240 million US voters within a 12-hour window requires approximately 5,556 ballot submissions per second throughout the day. No reviewed system has maintained this throughput concurrently with full cryptographic overhead—including ZKP verification, biometric authentication, and homomorphic tally accumulation—under adversarial network conditions.

9.2 Coercion Resistance

Coercion resistance can be enforced in traditional polling stations through physical isolation. In remote electronic voting, no cryptographic substitute has been successfully adapted for blockchain environments without introducing prohibitive usability or trust-setup requirements. The fake-credential approaches of the Civitas and JCJ coercion-resistant systems have not been operationalised in blockchain contexts.

9.3 Voter Privacy vs. Accountability

Even when vote content is cryptographically concealed, blockchain transaction metadata—including precise voting timestamps, network origin addresses, and transaction graph relationships—may permit adversaries to infer voter identity through traffic analysis. Proposed mitigations such as Tor integration, stealth address protocols, and vote-token mixing introduce additional complexity.

9.4 Accessibility and the Digital Divide

Any voting system that requires reliable broadband internet access, a modern smartphone or personal computer, and compatible biometric hardware will systematically exclude populations lacking these resources—an

unacceptable equity outcome for a democratic electoral application. Hybrid architectures combining blockchain-based auditability with accessible physical voting infrastructure offer a pragmatic path.

9.5 Smart Contract Upgradability

Electoral systems must remain functional and legally compliant for decades. Proxy-based upgrade patterns—such as Transparent Proxy and UUPS—allow contract logic to be replaced while preserving storage state, but introduce upgrade authority roles that create centralisation risks and potential attack vectors.

9.6 Regulatory and Legal Framework

Blockchain-based systems must satisfy requirements that may include mandatory paper audit trails, defined chain-of-custody procedures, specific voter registration processes, and formal result certification mechanisms. No comprehensive international legal standard for blockchain-based voting currently exists.

9.7 Post-Quantum Security Timeline

The transition of blockchain-based voting infrastructure to post-quantum cryptographic standards encompasses voter key re-enrollment, smart contract upgrades, infrastructure replacement, and backward-compatibility management. Given that cryptographically relevant quantum computers are estimated to emerge within a 10-to-20-year horizon, migration planning should begin well in advance.

Figure 5 illustrates the current estimated research maturity across the key challenge areas identified above:

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

Figure 5: Research Maturity by Challenge Area
(estimated based on reviewed literature)

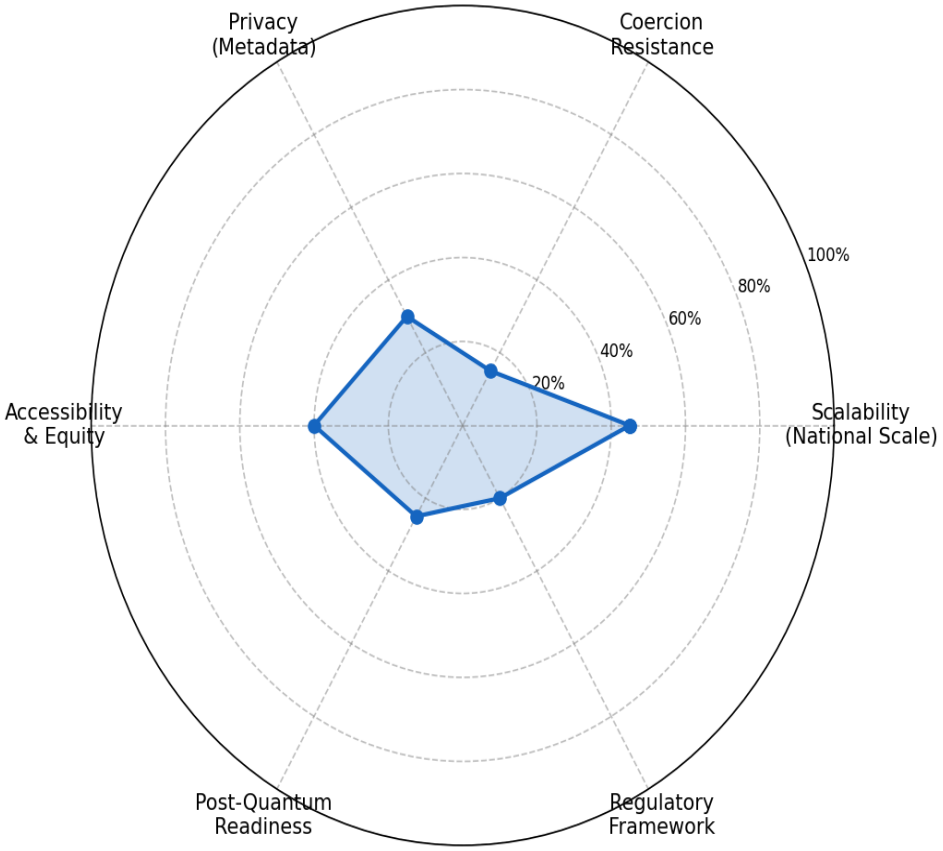

Figure 5: Research Maturity by Challenge Area (estimated based on reviewed literature)

10. Proposed Reference Architecture

10.1 Architectural Overview

Drawing on the reviewed literature and the open challenges identified above, we propose a five-layer reference architecture for a production-grade blockchain-based electronic voting system. Figure 4 illustrates the architecture:

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

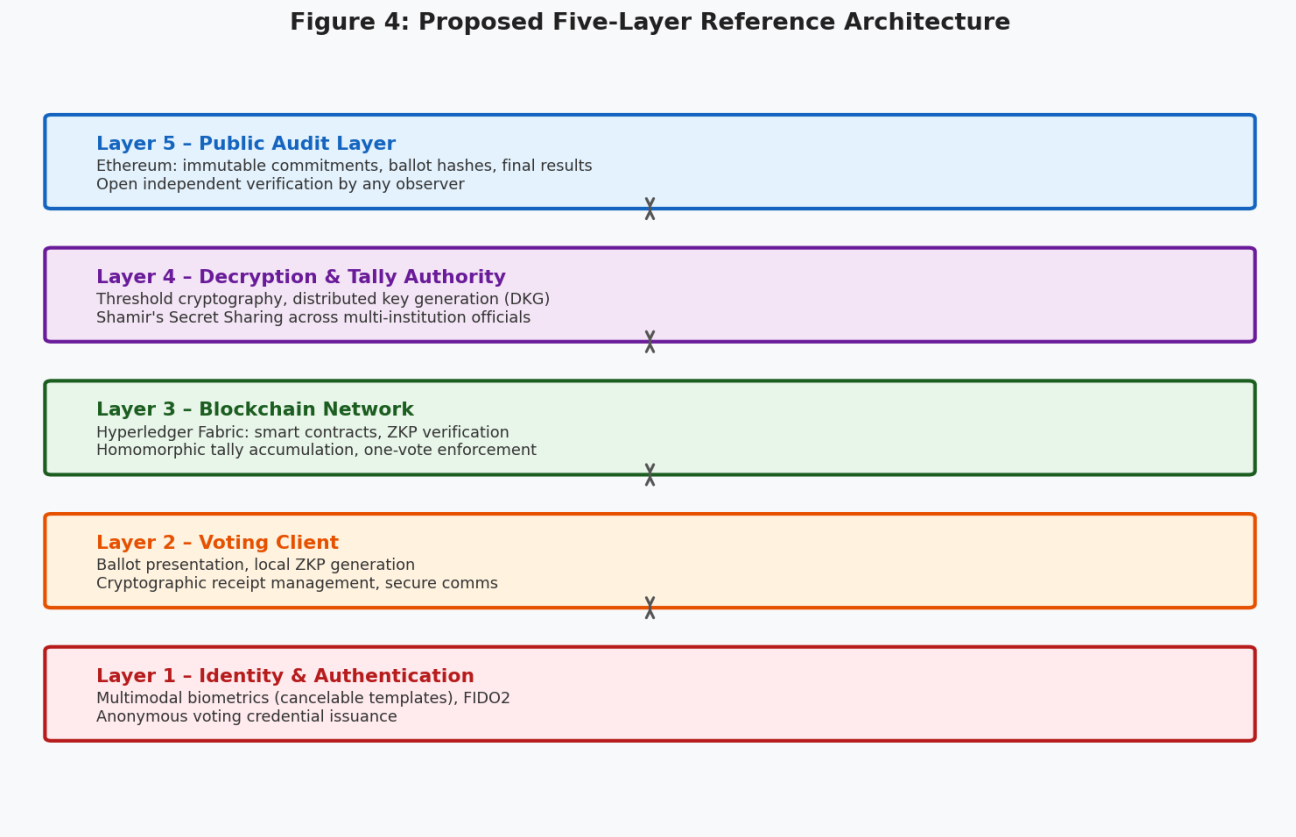

Figure 4: Proposed Five-Layer Reference Architecture

Each layer encapsulates a distinct set of responsibilities:

- Layer 1 – Identity and Authentication: multimodal biometric verification using cancelable template protection, integration with national identity databases, FIDO2-compliant local biometric verification, and issuance of anonymous cryptographic voting credentials.
- Layer 2 – Voting Client: ballot presentation, local generation of zero-knowledge ballot validity proofs, cryptographic receipt management, and secure communication with the blockchain network layer.
- Layer 3 – Blockchain Network: a permissioned blockchain (Hyperledger Fabric) receiving and validating ballot submissions, enforcing election rules through smart contracts, and accumulating an encrypted running tally using homomorphic operations.
- Layer 4 – Decryption and Tally Authority: a threshold cryptography layer jointly operated by election officials from multiple independent institutions, responsible for distributed key generation, threshold decryption, and publication of the final plaintext result.
- Layer 5 – Public Audit Layer: a public blockchain (Ethereum) storing immutable cryptographic commitments to election configuration parameters, ballot hashes, and final results.

10.2 Security Properties

The proposed architecture simultaneously satisfies seven core security properties:

- Completeness: every eligible voter who successfully authenticates and submits a valid ballot is counted in the final tally.

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

- Soundness: ineligible voters cannot cast ballots, and no eligible voter can cast more than one ballot.
- Ballot Secrecy: no party—including election authorities—can determine how any individual voter voted.
- Coercion Resistance: voters can re-vote within the election window, with only the final submission counted.
- Universal Verifiability: any external observer can independently verify that the published tally is the correct result.
- Individual Verifiability: each voter can confirm their ballot was included in the final tally.
- Robustness: the system continues to operate correctly even if a minority of election authority nodes fail, behave incorrectly, or are compromised.

10.3 Implementation Roadmap

A staged implementation approach is recommended: begin with small-scale institutional elections (university student unions, corporate shareholder meetings) to validate cryptographic and biometric components; progress to municipal or regional elections to test infrastructure at moderate scale; and pursue full national deployment only after independent security audits by multiple parties, formal regulatory approval, and sustained accessibility review involving representative voter populations.

12. Global Pilot Deployments and Real-World Case Studies

Beyond theoretical and laboratory-scale proposals, a growing number of real-world pilots and limited deployments have tested blockchain-based voting in operational electoral contexts. These deployments provide valuable empirical data on the practical challenges of adoption, the importance of voter education, and the regulatory hurdles that academic proposals frequently underestimate. This section surveys the most significant pilots documented in the reviewed literature and supplementary grey literature sources.

12.1 West Virginia Overseas Military Voting Pilot (2018)

In 2018, the state of West Virginia conducted the first blockchain-based voting pilot for overseas military personnel in a United States federal election, using the Voatz mobile application built on a private permissioned blockchain. Approximately 144 voters across 24 countries participated. While the pilot demonstrated that blockchain-based mobile voting could be operationally feasible, a subsequent independent security audit conducted by researchers at the Massachusetts Institute of Technology in 2020 identified serious vulnerabilities in the Voatz platform, including susceptibility to server-side manipulation, insufficient anonymisation of voter choices, and inadequate protection against malicious infrastructure operators. The West Virginia experience highlighted a critical lesson: operational feasibility does not imply cryptographic soundness, and independent pre-deployment security audits are a non-negotiable prerequisite for any electoral application.

12.2 Sierra Leone Agora Blockchain Voting (2018)

In March 2018, the Swiss-based organisation Agora recorded results from the Western province of Sierra Leone's presidential election on a public blockchain, providing an independently verifiable parallel tally. Importantly, the official results were determined by the conventional paper-based process; the blockchain record was a supplementary transparency mechanism rather than a replacement for the official count. This conservative deployment model—using blockchain as an auditability layer on top of existing processes rather than as a replacement—has since been recommended by several electoral integrity researchers as the most viable near-term adoption pathway. The Sierra Leone deployment demonstrated that even a read-only

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

blockchain record can meaningfully improve the transparency and verifiability of election results without requiring a wholesale overhaul of existing electoral infrastructure.

12.3 Moscow City Duma Election (2019)

The 2019 Moscow City Duma election incorporated a blockchain-based remote voting system for approximately 11,000 registered online voters. Prior to the election, a French security researcher publicly disclosed a critical vulnerability in the system's cryptographic implementation: the encryption key was insufficiently large, allowing individual votes to be decrypted in real time. Despite this disclosure, the election proceeded with a patched but incompletely audited system. The Moscow case illustrates two persistent challenges: the difficulty of conducting meaningful public cryptographic review under time pressure, and the political complexity of halting or delaying an election once a blockchain-based system has been officially announced. These dynamics have led researchers to advocate for extended public audit periods of at least six months prior to any live electoral deployment.

12.4 University and Corporate Governance Pilots

Several universities and corporate entities have deployed blockchain-based voting for internal governance decisions, providing a lower-stakes environment for empirical evaluation. The VoteChain Biometric pilot described in Section 3.4, conducted at a higher-education institution with 2,400 participants, is one such example. Similarly, multiple corporate annual general meetings in Switzerland, Estonia, and South Korea have used permissioned blockchain platforms for shareholder voting, reporting improvements in vote counting speed and audit trail completeness compared to traditional proxy voting mechanisms. These smaller-scale deployments consistently confirm that system usability, voter authentication reliability, and administrative tooling are as important to deployment success as the underlying cryptographic architecture.

13. Ethical, Legal, and Governance Considerations

The deployment of blockchain-based voting systems raises ethical, legal, and governance questions that extend well beyond the technical domain. This section examines the most critical non-technical dimensions that system designers, policymakers, and electoral authorities must address before blockchain-based voting can be considered a credible replacement for or supplement to established electoral processes.

13.1 Voter Privacy and Data Protection Law

The immutability of blockchain records, which is a core security property for electoral integrity, creates a direct tension with the right to erasure enshrined in data protection frameworks such as the European Union's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection Act (2023). If any personal data—including transaction metadata, cryptographic commitments, or biometric template references—is recorded on-chain, it may be legally impossible to honour a data subject's erasure request without invalidating the electoral audit trail. Reviewed proposals have addressed this tension in several ways: storing only cryptographic hashes of personal data on-chain while maintaining off-chain personal data in a deletable form; using zero-knowledge proofs that allow verification without any personal data appearing on the ledger; and deploying private or consortium blockchains where governance structures can authorise node-level data deletion under judicial order. No fully satisfactory general solution has emerged, and jurisdictional variation in data protection law means that a system compliant in one country may be legally non-deployable in another.

13.2 Algorithmic Accountability and Auditability

International Journal of Convergent Technologies and Future Systems (IJCTFS)
Website: https://www.maulikavyanshufoundation.org/IJCTFS/index.php
mail: maulikavyanshuijctfs@gmail.com | kavyanshufoundation@gmail.com
Volume 02 Issue-03 May-June 2026 ISSN NO: 3108-1312

Democratic legitimacy requires not only that an election produces a correct result, but that the process by which the result was produced is comprehensible and verifiable to non-specialist observers, including losing candidates, civil society organisations, and ordinary members of the public. Conventional paper-based voting achieves this through physical transparency: observers can watch ballots being counted. Blockchain-based systems replace physical transparency with mathematical transparency, but this substitution is only effective if the cryptographic proofs can be independently verified by parties with the requisite technical expertise. The current shortage of qualified cryptographic auditors, combined with the complexity of zero-knowledge proof systems and threshold cryptography protocols, means that genuine public verifiability remains more aspirational than actual in most proposed systems. Bridging this expertise gap through investment in accessible verification tools, plain-language audit reports, and regulatory capacity building is therefore as important as the underlying technical architecture.

13.3 Governance of Decentralised Electoral Infrastructure

Permissioned blockchain platforms require governance structures that define who may join the network as a validating node, who controls smart contract upgrades, and how disputes about ledger state are resolved. In an electoral context, these governance decisions are inherently political: concentrating node operation among a small number of government agencies may replicate the centralisation risks of existing systems, while distributing nodes across independent civil society organisations, international observers, and academic institutions introduces coordination complexity and potential for disagreement. The reviewed literature has not yet produced a widely accepted governance model for electoral blockchain networks. Drawing on analogies from international election observation frameworks, intergovernmental treaty mechanisms, and multi-stakeholder internet governance institutions may offer productive directions for future work in this area.

13.4 Environmental and Infrastructure Sustainability

Public blockchain networks based on Proof-of-Work consensus mechanisms, most notably Ethereum prior to its 2022 transition to Proof-of-Stake, have been widely criticised for their substantial energy consumption. Although the reviewed voting proposals predominantly favour permissioned platforms with energy-efficient consensus algorithms such as PBFT and Raft, the environmental credentials of any proposed system must be explicitly evaluated as part of the deployment feasibility assessment. Beyond energy consumption, the long-term sustainability of electoral blockchain infrastructure raises questions about hardware lifecycle management, software maintenance obligations, vendor dependency, and the capacity of electoral management bodies to operate and audit increasingly complex technical systems across election cycles that may span decades.

14. Future Research Directions

Based on the gaps and limitations identified throughout this review, the following research directions are considered the highest priority for advancing the field toward practical, trustworthy, and inclusive blockchain-based electoral systems.

Coercion-Resistant Remote Voting Protocols. Developing cryptographically sound coercion resistance for internet-based blockchain voting remains the field's most technically challenging open problem. Future research should explore adaptations of the JCJ and Civitas frameworks that are compatible with blockchain ledger semantics, as well as novel anonymous credential schemes that allow voters to invalidate coerced votes without revealing their true preference to a coercer.

Post-Quantum Migration Pathways. Concrete migration plans, prototype implementations, and performance benchmarks for post-quantum replacements of existing elliptic-curve and RSA-based components are urgently needed. Research should specifically address the performance implications of lattice-based signature schemes

such as CRYSTALS-Dilithium within smart contract environments, where gas costs and verification latency are constrained.

Accessibility-First System Design. Systematic user research with populations including elderly voters, voters with disabilities, and voters in low-connectivity environments is largely absent from the reviewed literature. Future work should apply universal design principles from the outset of system development, evaluate hybrid architectures that combine blockchain-based auditability with accessible physical interfaces, and develop standardised accessibility evaluation frameworks specific to electronic voting systems.

International Audit and Certification Standards. The absence of internationally recognised certification standards for blockchain-based voting systems is a significant barrier to adoption. Drawing on existing frameworks such as the Common Criteria for IT security evaluation and the IEEE Standards for Electronic Voting Systems, future work should contribute to the development of modular certification criteria that can be applied to the blockchain, smart contract, cryptographic, and biometric layers of a voting system independently, enabling incremental certification as individual components mature.

Large-Scale Adversarial Stress Testing. No reviewed system has undergone a realistic adversarial stress test at national-election scale with the full cryptographic and biometric stack active simultaneously. Future research should establish shared benchmarking environments, adversarial testing methodologies, and open datasets that allow independent researchers to evaluate competing proposals under comparable and realistic conditions.

15. Conclusion

This review has systematically examined the state of research in blockchain-based electronic voting, with focused attention on the integration of smart contract logic, multi-layer cryptographic protection, and biometric voter authentication. The trajectory of the field — progressing from early Ethereum prototypes to sophisticated hybrid architectures that combine the performance of permissioned blockchains with the auditability of public ledgers, and pairing zero-knowledge proof privacy with end-to-end verifiability — reflects genuine and sustained technical advancement over the past decade.

The principal insight emerging from this analysis is that no individual component — whether blockchain, cryptography, or biometrics — is alone sufficient to build a trustworthy digital voting system. It is their deliberate, co-designed integration that enables the simultaneous achievement of properties that appear in tension: public transparency alongside individual ballot secrecy, mathematical verifiability alongside voter anonymity, and decentralised governance alongside practical operational performance.

The most significant barriers that remain are not primarily theoretical but practical: engineering systems that operate reliably at national scale, ensuring digital accessibility for all segments of the voter population, navigating fragmented regulatory landscapes, and sustaining decentralised infrastructure across multi-year election cycles. Priority areas for future work include developing coercion-resistant remote voting protocols, completing the migration to post-quantum cryptographic standards, adopting accessibility-first design methodologies from the earliest stages of system development, and establishing internationally recognised certification frameworks for blockchain-based electoral systems.

References

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[2] Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. Ethereum Yellow Paper.

[3] Adida, B. (2008). Helios: Web-based open-audit voting. In Proceedings of the 17th USENIX Security Symposium (pp. 335–348).

[4] McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. In Financial Cryptography and Data Security (FC 2017), LNCS 10322 (pp. 357–375).

[5] Hardwick, F. S., Akram, R. N., Markantonakis, K., & Watters, P. (2018). E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. IEEE IoT Conference.

[6] Zhang, S., Wang, L., & Xiong, H. (2019). Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability. International Journal of Information Security, 19(3), 323–341.

[7] Abuidris, Y., Hassan, R., & WStore, T. (2019). A survey of blockchain based on e-voting systems. In Proceedings of the 2nd International Conference on Computing and Big Data.

[8] Sadia, K. et al. (2019). Blockchain based secured e-voting by using the assistance of smart contract. In 2019 International Conference on Computer and Information Technology.

[9] Groth, J. (2016). On the size of pairing-based non-interactive arguments. In Advances in Cryptology – EUROCRYPT 2016, LNCS 9666 (pp. 305–326). Springer.

[10] NIST. (2020). Recommendation for key management: Part 1 – General (SP 800-57). National Institute of Standards and Technology.

[11] NIST. (2024). Post-quantum cryptography standards: CRYSTALS-Kyber and CRYSTALS-Dilithium. National Institute of Standards and Technology.

[12] Kumar, A., Singh, R., & Vatsa, M. (2023). Multimodal biometric fusion using fingerprint and iris for high-assurance identity verification. IEEE Transactions on Information Forensics and Security, 18, 1124–1137.

[13] Szabo, N. (1997). Formalising and securing relationships on public networks. First Monday, 2(9).

[14] Paillier, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. In Advances in Cryptology – EUROCRYPT 1999, LNCS 1592 (pp. 223–238). Springer.

[15] Ben-Sasson, E. et al. (2014). Succinct non-interactive zero knowledge for a von Neumann architecture. In USENIX Security Symposium (pp. 781–796).

[16] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612–613.

[17] Pedersen, T. P. (1991). Non-interactive and information-theoretic secure verifiable secret sharing. In Advances in Cryptology – CRYPTO 1991, LNCS 576 (pp. 129–140). Springer.

[18] Juels, A., Catalano, D., & Jakobsson, M. (2005). Coercion-resistant electronic elections. In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (pp. 61–70).

[19] Adida, B., de Marneffe, O., Pereira, O., & Quisquater, J.-J. (2009). Electing a university president using open-audit voting: Analysis of real-world use of Helios. In Proceedings of the 2009 Conference on Electronic Voting Technology.

[20] Cramer, R., Gennaro, R., & Schoenmakers, B. (1997). A secure and optimally efficient multi-authority election scheme. In Advances in Cryptology – EUROCRYPT 1997, LNCS 1233 (pp. 103–118). Springer.

[21] Zaghloul, E., Li, T., Mutka, M. W., & Ren, J. (2020). E-voting systems: A survey on different security challenges and countermeasures. IEEE Transactions on Consumer Electronics, 66(4), 378–397.

[22] Pawlak, M., Poniszewska-Maranda, A., & Kryvinska, N. (2018). Towards the Blockchain technology for network communication systems. Procedia Computer Science, 130, 954–959.

[23] Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. Journal of Cryptology, 3(2), 99–111.

[24] Chaum, D. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2), 84–90.

[25] Bernhard, D., Cortier, V., Galindo, D., Pereira, O., & Warinschi, B. (2015). A comprehensive analysis of game-based ballot privacy definitions. In Proceedings of the 2015 IEEE Symposium on Security and Privacy (pp. 499–516).

[26] Cortier, V., Gaudry, P., & Glondu, S. (2014). Belenios: A simple private and verifiable electronic voting system. In Foundations & Practice of Security, LNCS 8930 (pp. 214–233). Springer.

[27] Khader, D., Ryan, P. Y. A., Smyth, B., & Hao, F. (2012). Preventing vote selling with deniable receipts. In Proceedings of the 2012 European Workshop on Security and Privacy in Ad-hoc and Sensor Networks.

[28] Ayed, A. B. (2017). A conceptual secure blockchain based electronic voting system. International Journal of Network Security & Its Applications, 9(3), 1–9.

[29] Hanifatunnisa, R., & Rahardjo, B. (2017). Blockchain based e-voting recording system design. In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA).

[30] Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. IEEE Software, 35(4), 95–99.

[31] Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983–986).

[32] Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a blockchain based e-voting system. In Proceedings of KMIS 2018: 10th International Conference on Knowledge Management and Information Systems.

[33] Li, Y., Susilo, W., Yang, G., Yu, Y., Du, X., & Guizani, M. (2019). Toward privacy and regulation in blockchain-based cryptocurrencies. IEEE Network, 33(5), 111–117.

[34] Zhao, Z., & Chan, T. H. H. (2015). How to vote privately using bitcoin. In International Conference on Information and Communications Security, LNCS 9543 (pp. 82–96). Springer.

[35] Baum, C., Damgard, I., Toftdahl, M., & Zottarel, A. (2021). Post-quantum UC-secure oblivious polynomial evaluation and applications. In Public-Key Cryptography – PKC 2021, LNCS 12711 (pp. 217–246). Springer.

[36] Clarkson, M. R., Chong, S., & Myers, A. C. (2008). Civitas: Toward a secure voting system. In 2008 IEEE Symposium on Security and Privacy (pp. 354–368).

[37] Buchman, E., Kwon, J., & Milosevic, Z. (2018). The latest gossip on BFT consensus. arXiv preprint arXiv:1807.04938.

[38] Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In Proceedings of the 3rd Symposium on Operating Systems Design and Implementation (OSDI), Vol. 99 (pp. 173–186).

[39] Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194.

[40] Demirag, I., & Gosovic, M. (2019). Blockchain for public sector accountability. Accounting Forum, 43(4), 376–395.

[41] MIT Digital Currency Initiative. (2020). Voatz security analysis. MIT CSAIL Technical Report, Massachusetts Institute of Technology.

[42] Agora. (2018). Agora's blockchain-based voting in Sierra Leone. Agora Technical White Paper. https://www.agora.vote