Abstract
Blockchain technology has emerged as a promising foundation for next-generation electronic voting (e-voting) systems by offering properties such as immutability, transparency, and distributed trust that align closely with democratic requirements like integrity, verifiability, and auditability. Existing research spans broad architectural surveys of blockchain-based e-voting, biometric-enabled authentication mechanisms, hybrid on-/off-chain storage models, and smart contract–driven decentralized applications –. These works collectively indicate that while blockchain can mitigate traditional threats such as ballot tampering, booth capturing, and identity theft, it simultaneously introduces new challenges related to scalability, cybersecurity, cost, and regulatory integration, –. This survey synthesizes and categorizes blockchain-based e-voting approaches into three main classes: biometric-enabled systems, hybrid/cost-optimized systems, and Ethereum/smart contract–based systems –, . For each class, we analyze design goals, underlying technologies, security and privacy properties, and operational constraints, followed by a comparative analysis across usability, performance, cost, and deployment feasibility. We further discuss open challenges in scalability, privacy, security, and governance, emphasizing the unresolved tension between nationwide deployment requirements and the limitations of existing blockchain infrastructures and legal frameworks, , . The survey concludes that, although several proof-of-concept implementations demonstrate technical feasibility, large-scale adoption of blockchain-based e-voting depends on addressing scalability bottlenecks, biometric robustness (including deep fake threats), sustainable cost models, and comprehensive legal and institutional regulation .

I. Introduction

In the era of digitization the very core of democratic countries 'elections' still rely on paper ballot systems. Paper ballots have been around long enough and have provided efficient results as well but as the era has changed, better alternatives to the traditional paper ballots exist. The reason government may hesitate to bring in the replacements could be that the wider public has been accustomed to this system for more than decades now and changing this would result in government educating the public on the substitute they would like to bring forth. Paper ballots do have cons as well and the reasons we should be looking for an alternative, that being, too much reliability on people auditing the ballots, booth capturing, environmental effects due to use of paper, identity thefts and many more. Recently, researchers are investigating the possibility of blockchain being implemented in the democratic process due to many of its properties that align with the core principles of an election, still not perfect but this technology may bring advancements to the election process and uphold the core values of democracy, some of them being authenticity, transparency, security etc. This survey paper in brief compares various blockchain implementation methodologies that exist in theory and the ones that have been implemented, and identifies the gap that still exists and provides a comparative study on these methodologies.

II. Background and Related Work

A. Traditional Voting and E-Voting Systems

Conventional paper-based voting remains the dominant mechanism for conducting elections in many democratic nations due to its perceived simplicity, transparency, and long-standing institutional acceptance. However, paper ballots are vulnerable to a range of issues, including ballot stuffing, booth capturing, physical ballot destruction, and dependence on large-scale human auditing, which

can introduce both error and bias. Electronic voting machines (EVMs) and web-based e-voting were proposed to improve efficiency and reduce human error, yet they often centralize trust in election authorities or vendors, creating single points of failure and raising concerns about insider attacks, malware, and opacity of proprietary software. Traditional e-voting systems typically rely on centralized databases and authentication servers, which, if compromised, can threaten voter privacy, enable large-scale manipulation, and undermine public trust in election results.

B. Blockchain Fundamentals for E-Voting

Blockchain is a distributed ledger technology where transactions are grouped into blocks that are cryptographically linked, providing tamper-evident and append-only properties. Consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS) ensure that participating nodes agree on the state of the ledger without relying on a central authority, although each mechanism carries different trade-offs in terms of speed, energy consumption, and security, . For e-voting, blockchain's immutability and transparency can facilitate end-to-end verifiability, allowing voters and auditors to confirm that ballots were recorded and tallied correctly without exposing the association between voter identities and votes, . Smart contracts further enable programmable election logic, such as eligibility checks, vote casting, tallying, and automated result publication, thereby reducing manual intervention and the risk of tampering in intermediate stages .

C. Blockchain-Based Voting: Survey and Public vs. Private Models

Jafar et al. present a general survey of blockchain-based e-voting systems, identifying how blockchain can enhance transparency and integrity while highlighting new risks related to cybersecurity and resource intensity. Their analysis stresses that PoW-based platforms can be too slow and resource-demanding for national-level elections, particularly when transaction volumes peak during voting periods, . Parallel work on blockchain in public sector services notes a fundamental design choice between public blockchains (e.g., Bitcoin-like) and permissioned or consortium blockchains controlled by authorized entities . For national elections, consortium blockchains—where only designated government or institutional nodes validate blocks—are argued to better satisfy performance, privacy, and governance requirements than fully public networks, which may expose sensitive metadata and rely on economically driven security incentives . These foundational studies motivate the more specialized voting architectures surveyed in subsequent sections, which build upon different combinations of consensus models, smart contracts, biometrics, and hybrid storage schemes .

III. Categorization of Methodologies

This section categorizes the examined works into three primary methodological classes based on their dominant design focus: biometric-enabled systems, hybrid/cost-optimized architectures, and Ethereum/smart contract–based implementations.

A. Biometric-Enabled Blockchain E-Voting Systems

Biometric-enabled systems integrate facial recognition or similar modalities with blockchain-based backends to strengthen voter authentication and mitigate identity theft. One line of work proposes a decentralized e-voting system in which voter identity is verified using face recognition techniques before a ballot is submitted to a blockchain ledger . In this design, an Android-based front-end application captures the voter's facial image via a webcam, then employs algorithms such as Haar Cascade or convolutional neural networks (CNNs) to match the live capture against a pre-registered

identity database, such as Aadhaar or a comparable national ID repository . Upon successful authentication, the voter is allowed to cast a vote, which is then recorded on a multichain-based blockchain; Python is used for implementing the face detection pipeline, providing a modular architecture where biometric verification and ledger operations are logically separated .

The advantages of this approach include reduced risk of impersonation, mitigation of booth capturing, and more robust enforcement of “one person, one vote,” as facial biometrics are harder to duplicate than simple credentials or tokens . At the same time, the system’s reliability is highly dependent on environmental factors such as camera quality, illumination conditions, and network bandwidth, which can degrade recognition accuracy or make the system inaccessible in low-resource settings . Another contribution extends biometric-based voting by adding a deep fake detection layer to address emerging threats wherein adversaries use synthetic media to spoof facial recognition systems . This framework first checks whether the captured face is genuine using a deep fake detection model trained on benchmark datasets (e.g., Kaggle), and only when the input is classified as authentic does the system proceed to standard face recognition and voting .

The deep fake–aware system demonstrates 97.36% accuracy in voter authentication on a Kaggle dataset, indicating strong potential for resisting synthetic identity attacks . Votes are recorded via smart contracts on the blockchain, ensuring immutability and transparent tallying while the biometric and liveness checks safeguard against fraudulent ballot casting . However, such systems must carefully manage privacy, as storing or linking biometric templates to on-chain identifiers could expose sensitive information if not handled through privacy-preserving encoding, off-chain storage, or cryptographic anonymization techniques , . Collectively, these biometric-enabled approaches emphasize secure voter authentication as a cornerstone of trustworthy blockchain-based e-voting.

B. Hybrid and Cost-Optimized Blockchain Voting Architectures

A second category focuses on addressing storage and transaction-cost challenges by combining on-chain and off-chain components. One remote and cost-optimized voting system proposes a hybrid storage architecture in which only “cardinal data” such as hashes of votes are stored directly on the blockchain, while heavy data—such as full encrypted ballots or supplementary metadata—is kept off-chain, for example in distributed storage systems like the InterPlanetary File System (IPFS) . This design significantly reduces the amount of data written to the chain, thereby decreasing gas costs and improving scalability without sacrificing the ability to verify ballot integrity, since hashes can be used to confirm that off-chain content has not been altered .

The system also integrates smart contracts with artificial intelligence mechanisms to optimize transaction verification and potentially prioritize or batch processing, which can further decrease operational costs and latency . By decoupling storage and computation, hybrid architectures can support larger electorates and more complex ballot structures than fully on-chain designs, while retaining verifiability through cryptographic linkages between on-chain hashes and off-chain encrypted records . Nonetheless, hybrid schemes introduce new dependencies and trust assumptions regarding off-chain infrastructure availability, content-addressable storage reliability, and secure key management for encrypting and decrypting ballots . These trade-offs position hybrid/cost-optimized systems as promising candidates for resource-constrained electoral environments, provided that appropriate redundancy and security measures are enforced.

C. Ethereum and Smart Contract–Based E-Voting Systems

A third class of methodologies leverages public or semi-public smart contract platforms, particularly Ethereum, to implement decentralized voting applications (DApps). One system proposes a smart

voting platform built using the Ethereum network, where the election logic is encoded in Solidity-based smart contracts and voter identities are managed through MetaMask wallets . In this architecture, the voting process typically involves a user login step mediated by MetaMask, which verifies the voter's wallet address and associates it with eligibility records; upon successful verification, the user casts a vote through the DApp interface, triggering a smart contract function that records the vote as a transaction on the Ethereum blockchain . Once mined and confirmed, the transaction becomes part of the immutable ledger, and the smart contract can later compute and expose election results in a transparent manner .

This Ethereum-based design benefits from the platform's mature tooling, broad node infrastructure, and well-established security assumptions, making it suitable for prototyping and limited-scale elections . However, gas fees on the Ethereum mainnet represent a significant barrier to wide-scale adoption, as voting involves a potentially large number of write operations, each incurring transaction costs that can fluctuate with network congestion . To mitigate these issues, variants may consider deploying on permissioned Ethereum networks, layer-2 scaling solutions, or sidechains, but such choices affect decentralization properties and may require additional governance structures , . Beyond Ethereum, other works explore PoW-based blockchain platforms combined with machine learning to enhance transaction security and anomaly detection in voting patterns . In these systems, votes are validated via PoW consensus, providing strong tamper-resistance at the expense of high computational overhead and latency, while machine learning modules monitor network activity to identify suspicious IP addresses or abnormal voting patterns that might signal coordinated attacks or coercion . Together, these smart contract and PoW-based approaches highlight the trade-off between leveraging existing public blockchain ecosystems and designing domain-specific, permissioned infrastructures tailored to electoral needs.

IV. Comparative Analysis of Approaches

This section compares the surveyed methodologies along several dimensions, including authentication, storage model, consensus mechanism, cost profile, and deployment feasibility.

A. Qualitative Comparison

The different approaches can be contrasted as follows:

Aspect	**Biometric-enabled systems ,**	**Hybrid / cost-optimized systems**	**Ethereum / smart contract systems ,**	**Public vs. consortium design insights**
Primary goal	Strong voter authentication, prevent identity theft and booth capturing ,	Reduce on-chain storage and gas cost while preserving integrity	Leverage existing DApp infrastructure and smart contracts for transparent voting ,	Select governance model and trust structure suitable for national elections
Authentication	Face recognition, optionally deep fake detection;	Typically external to storage model;	Wallet-based identity via MetaMask or	Emphasizes institutional control and node

Aspect	Biometric-enabled systems ,	Hybrid / cost-optimized systems	Ethereum / smart contract systems ,	Public vs. consortium design insights
	linked to national IDs ,	can integrate standard or biometric schemes	similar; may integrate off-chain KYC	authorization rather than specific biometrics
Storage model	Full or partial vote data on-chain; depends on implementation ,	Hashes on-chain, encrypted ballots off-chain (e.g., IPFS)	Full transactions on-chain; vote data recorded in smart contract state ,	Varies; often permissioned ledgers for performance and privacy
Consensus / platform	Multichain or similar; not always specified in detail ,	Smart contracts with AI-assisted verification; underlying chain unspecified or generic	Ethereum PoW/PoS-style network, or PoW-based custom chain plus ML anomaly detection ,	Advocates consortium/permissioned chains for electoral contexts
Security focus	Prevent impersonation and deep fake–based attacks; ensure one vote per person ,	Maintain integrity while minimizing cost; rely on cryptographic hashes and off-chain security	Leverage blockchain immutability and ML anomaly detection; address transaction-level manipulation ,	Address system-wide trust, cybersecurity risks, and regulatory compatibility
Cost / scalability	Dependent on biometric computation and underlying chain; network and hardware constraints ,	Optimized gas and storage usage; better suited to large electorates	Potentially high gas fees; mainnet unsuitable for very large national elections ,	Highlights infrastructure and resource constraints for nationwide deployments

As the table indicates, biometric-enabled systems primarily enhance the front-end authentication process, hybrid systems optimize back-end storage and cost, and Ethereum-based DApps focus on programmability and leveraging existing ecosystems –. Survey and public-sector studies provide overarching guidance on consensus choices, governance, and infrastructural requirements, arguing for consortium blockchains in national-level deployments to balance performance and control.

B. Strengths and Limitations

Biometric-enabled blockchain voting systems provide strong guarantees against impersonation and multiple voting, as facial recognition tightly links ballots to unique individuals , . The inclusion of deep

fake detection significantly improves resilience to modern synthetic media attacks, thereby strengthening the trustworthiness of biometric authentication . Nevertheless, these systems face challenges in terms of false positives/negatives, environmental sensitivity, and privacy concerns associated with handling biometric data, particularly if any part of the biometric template or its linkage to on-chain identities is exposed , .

Hybrid/cost-optimized approaches excel in addressing the high storage and gas costs associated with fully on-chain designs by moving large encrypted ballot data off-chain and storing only hashes on the blockchain . This strategy enables better scalability and cost-effectiveness, making it more realistic for nationwide elections or frequent local ballots, especially when combined with AI-assisted verification to streamline transaction processing . However, these systems introduce complexity in ensuring that off-chain storage remains available, tamper-resistant, and properly synchronized with on-chain records, potentially requiring additional trust in the operators of off-chain infrastructure .

Ethereum and smart contract–based systems offer a flexible and expressive platform for implementing voting rules, eligibility checks, and automated tallying, and they benefit from robust tooling and a large developer community , . Yet, as highlighted by both implementation studies and broader surveys, PoW-based consensus and mainnet gas fees present significant obstacles for large-scale political elections, making such systems more appropriate for smaller or organizational contexts unless alternative scaling solutions are adopted, , . Survey work on blockchain for e-voting further underscores that cybersecurity risks, resource intensity, and lack of robust nationwide infrastructure remain unsolved, especially when considering heterogeneous network conditions and device capabilities across a country.

V. Challenges

Despite promising advances, several critical challenges remain in deploying blockchain-based e-voting systems at national or even regional scales. This section focuses on scalability, privacy and security, and cost.

A. Scalability and Performance

Scalability is a central bottleneck for blockchain-based e-voting, particularly when using PoW or other resource-intensive consensus mechanisms. Surveys and implementation studies report that PoW-based systems, while secure against double-spending and tampering, are too slow and computationally expensive for large-scale elections where millions of voters may cast ballots within a limited time window, . In PoW-based voting schemes, each vote corresponds to a transaction requiring network-wide validation and inclusion in a block, leading to high latency and potential throughput constraints when block times and maximum block sizes are fixed .

Hybrid systems offer one pathway to improved scalability by minimizing the volume of data stored on-chain, thereby reducing transaction size and associated validation overhead . By committing only hashes of ballots or aggregated results to the blockchain while holding the full encrypted data off-chain, these architectures can handle large electorates with less pressure on the underlying consensus mechanism . Nonetheless, national-scale deployment still demands robust network infrastructure, carefully tuned block parameters, and potentially the use of consortium or permissioned blockchains to achieve acceptable throughput, as emphasized in analyses of public versus private blockchain choices for public services.

B. Privacy and Security: Identity Theft, Deep Fakes, and Cyber Risks

Security in blockchain-based e-voting extends beyond ledger integrity to encompass voter authentication, resistance to coercion, and protection against modern cyber threats. Biometric-enabled systems aim to reduce identity theft and booth capturing by enforcing strong, person-specific authentication via facial recognition, preventing voters from delegating credentials or being impersonated by others . However, the rise of deep fake technologies creates new attack vectors, where adversaries might present synthetic video or images to fool face recognition systems into accepting unauthorized voters . The introduction of a deep fake detection layer is a direct response to this threat, providing an additional classification stage that can detect manipulated media and thus prevent fraudulent votes, with reported high accuracy on benchmark datasets .

Despite these advances, privacy remains a major concern, as biometric data is inherently sensitive and long-lived. Systems must ensure that biometric templates or their representations are stored securely, preferably off-chain and in encrypted or anonymized form, to prevent linkage between an individual's identity and their voting record , . Beyond biometrics, broader cybersecurity risks identified in surveys include potential vulnerabilities in smart contract code, network-level attacks on nodes or communication channels, and targeted attacks against consortium validators or government-operated nodes. PoW and other consensus mechanisms also expose systems to resource-based attacks, where adversaries attempt to accumulate sufficient hashing or stake power to influence the ledger, underscoring the need for robust governance and monitoring coupled with technical safeguards such as machine learning–based anomaly detection in voting traffic and node behavior.

C. Cost, Gas Fees, and Infrastructure Requirements

Cost is a further critical barrier to deploying blockchain-based voting at scale, particularly on public platforms that charge transaction fees. Ethereum-based voting systems incur gas fees for each transaction associated with voter authentication, vote casting, and result computation, making large elections financially prohibitive on the mainnet . These costs are subject to network congestion and gas price volatility, making it difficult for election authorities to predict or control total expenditure . While deploying on private Ethereum networks or sidechains can alleviate gas costs, such configurations reduce reliance on the economic security model of public chains and require separate governance and security assurances , .

Hybrid systems are specifically designed to reduce cost by minimizing on-chain storage, storing only small hashes while keeping large encrypted ballots off-chain, which significantly lowers transaction fees and storage requirements . Surveys of blockchain-based e-voting further note that beyond direct gas costs, nationwide adoption requires considerable investment in network infrastructure, node operation, hardware, and biometric capture devices, particularly in regions with limited digital connectivity, . Consequently, research highlights a gap between proof-of-concept prototypes, which demonstrate technical feasibility on limited scales, and the comprehensive infrastructural and financial commitments necessary to support legally binding national elections,

---

VI. Conclusion

Blockchain-based e-voting systems present a compelling vision for modernizing electoral processes by combining immutability, transparency, and distributed trust with advanced authentication mechanisms and programmable election logic –. The surveyed works demonstrate that core building blocks—biometric-enabled voter verification with face recognition and deep fake detection, hybrid on-/off-chain storage to optimize cost, and Ethereum or similar smart contract platforms for

transparent tallying—are technically viable and can address many weaknesses of traditional paper-based and centralized e-voting systems –. In particular, biometric systems target identity theft and booth capturing, hybrid architectures mitigate storage and gas costs, and smart contract–based DApps provide verifiable and automated election workflows, showing that essential technological capabilities already exist

However, comprehensive surveys and public-sector analyses emphasize that these advances have not yet resolved fundamental challenges in scalability, cybersecurity, infrastructure readiness, and regulatory integration at national scales, . PoW-based and mainnet-oriented designs face limitations in throughput and economic sustainability, while consortium blockchain models, though better aligned with governmental control and privacy, require clear legal frameworks and governance structures to ensure legitimacy and accountability, , . Moreover, handling biometric data securely and preserving voter privacy in the face of deep fake threats and sophisticated cyber attacks remains an open research problem, necessitating ongoing work in privacy-preserving cryptography, secure off-chain storage, and robust anomaly detection , , . Overall, while blockchain-based e-voting is poised to significantly enhance electoral integrity and transparency, its transition from experimental prototypes to nationwide deployment hinges on addressing scalability constraints, developing cost-effective and privacy-respecting architectures, and embedding these technical systems within coherent legal and institutional frameworks.

References

Jafar et al., “Blockchain for Securing Electronic Voting Systems: A Survey,” 2021.

“Decentralized E-Voting System using Blockchain,” International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET), 2025.

“Research on Blockchain E-voting based on Face Recognition & Deep Fake Detection,” IEEE, 2021.

“A Remote and Cost-Optimized Voting System,” IET Blockchain, 2022.

“Blockchain-based E-voting using Proof of Work and Machine Learning,” Research Paper, 2024.

“Smart Voting System using Ethereum and Solidity,” TIJER, 2024.

“CANCUM 2019 / King Saudi University Paper,” 2022.