Comparative Analysis of Blockchain-Based E-Voting Implementations: Biometric, Hybrid, and Ethereum-Based Approaches

Tamanna | Mudit Purswani
Department of Computer Science and Technology
Manipal University Jaipur

Abstract

Blockchain technology has emerged as one of the best possible systems for the implementation of 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 discusses many systems to implement blockchain like biometric-enabled authentication mechanisms, hybrid on-off-chain storage models, and smart contract–driven decentralized applications.These indicate that while blockchain can eliminate traditional threats such as ballot tampering, booth capturing, and identity theft, but it also presents major problems like scalability, cybersecurity, cost, and regulatory integration. This survey categorizes blockchain-based e-voting approaches into three main categories: biometric-enabled systems, hybrid/cost-optimized systems, and Ethereum/smart contract–based systems. For each, design goals, underlying technologies, security and privacy properties, and operational constraints are analyzed, and further a comparative analysis on usability, performance, cost, and deployment feasibility is discussed. We further discuss open challenges in scalability, privacy, security, and governance. The survey concludes that, although several implementations demonstrate that blockchain can be used as a platform for E-voting but, large-scale adoption of blockchain-based e-voting depends on addressing scalability problems, sustainable cost models, and many more.

I. Introduction

In the era of digitization the very core of democratic countries ‘elections’ still rely on paper ballot systems. Paper ballots and polling booths have been around long enough and have provided efficient results as well but as the era has changed, better alternatives to these system 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 and polling booth 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 simplicity, transparency, and existing 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 cause both error and bias. Electronic voting machines (EVMs) and web-based e-voting were introduced to improve efficiency and reduce human error, yet they put trust in election authorities or vendors, which creates a single point of failure and raises concerns about insider attacks and malware. Traditional e-voting systems rely heavily on centralized databases and servers, which can threaten voter privacy, cause large-scale vote manipulation, and weaken 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 a secured de-centralised system where every block that you add has to go through a consensus mechanism, such as Proof of Work (PoW) or Proof of Stake (PoS), ensuring that participating nodes agree on the state of the ledger without relying on a central authority, although each mechanism is different in terms of speed, energy consumption, and security. For e-voting, blockchain’s immutability and transparency can promote end-to-end verifiability, allowing voters and auditors to confirm that ballots were recorded and tallied correctly without relating voter identities with votes-which is one of the major concerns. Smart contracts further enable programmable election logic, such as eligibility checks, vote casting, tallying, and automated result publication, reducing manual intervention and the risk of tampering in intermediate stages.

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

Jafar et al. presents a general survey of blockchain-based e-voting systems, identifying how blockchain can improve transparency and integrity while also highlighting new risks related to cybersecurity and resource intensity. Their analysis points out that PoW-based platforms can be too slow and resource-demanding for national-level elections, especially when the number of transactions peak during voting. Parallel work on blockchain in public sector services notes a distinct design choice between public blockchains (e.g., Bitcoin-like) and permissioned blockchains controlled by authorized entities. For national elections, permissioned blockchains—where only designated nodes validate blocks—are said to have better performance, privacy, and governance requirements than fully public networks, which may expose sensitive data. These studies motivate more specialized voting architectures, surveyed in subsequent sections, which consist of 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 major 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 models with blockchain-based backends to strengthen voter authentication and reduce identity theft. This system proposes the idea where voter identity is verified using face recognition techniques before the ballot is submitted . 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(most preferable) or a comparable national ID . Upon successful authentication, the voter is allowed to cast a vote, which is then recorded on a multichain-based blockchain-multichain based blockchain tries to solve the issue of scalability- Further Python is used for implementing the face detection pipeline, providing an architecture where biometric verification and ledger operations are logically separated and the ledger operations are dependent on the verifiability and result of the biometric verification .

The advantages of this approach include reduced risk of identity theft, no more booth capturing, and more efficient 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 affect recognition accuracy or make the system inaccessible in low-resource settings. For further security, biometric-based voting can add a deep fake detection layer to protect against emerging threats. 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 and only when the input is classified as authentic the system proceeds 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 protecting against identity attacks . Votes are recorded via smart contracts on the blockchain, ensuring immutability and transparent tallying while the biometric and liveness checks protect against fraud 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 carefully through privacy-preserving encoding, off-chain storage, or cryptographic anonymization techniques. To sum it up, these biometric-enabled approaches emphasize secure voter authentication as a major part for a trustworthy blockchain-based e-voting system.

B. Hybrid and Cost-Optimized Blockchain Voting Architectures

The second category focuses on addressing storage and transaction-cost challenges by combining on-chain and off-chain components. A remote and cost-optimized voting system proposes a hybrid storage architecture in which only “cardinal data”(small size 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). IPFS produces a CID -a content based hash- which is further stored onto the chain , this makes sure that we have the record of the heavy data too but just not on chain, IPFS also ensure that if any tampering is done , the hash changes and can further be verified by comparing it to the on-chain hash. This design significantly reduces the amount of data written to the chain, thereby decreasing gas costs and improving scalability.

The system also integrates smart contracts with artificial intelligence mechanisms to verify transactions and prioritize processing, which help to decrease operational costs and latency. By separating storage and computation, hybrid architectures can support larger voters and more complex ballot structures than fully on-chain designs. They also retain verifiability through cryptographic linkages between on-chain hashes and off-chain encrypted records. Nonetheless, hybrid schemes introduce new problems and trust issues regarding availability of off-chain facility, storage reliability, and secure key management for encrypting and decrypting ballots. These systems are suitable for places with limited resources, as long as they have strong security and backup mechanisms.

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

A third category of methodologies uses public or semi-public smart contract platforms, particularly Ethereum, to implement decentralized voting applications (DApps).This 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. The voting process typically involves a user login step, MetaMask working as medium for it, which verifies the voter’s wallet address, 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 give election results in a transparent manner.

This Ethereum-based design benefits from the platform’s smart tools, great 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 large number of write operations, each transaction costs that can fluctuate with network congestion(traffic on the chain). To resolve these issues, a solution could be, 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(any false or unusual activity in the chain) . In these systems, votes are validated via PoW consensus, providing strong tamper-resistance at the expense of high computational overhead while machine learning modules monitor network activity to identify suspicious IP addresses or abnormal voting patterns. Together, these smart contract and PoW-based approaches highlight the exchanges between using existing public blockchain ecosystems and designing domain-specific, permissioned chains for the 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; linked to national IDs	Typically external to storage model; can integrate standard or biometric schemes	Wallet-based identity via MetaMask or similar; may integrate off-chain KYC	Emphasizes institutional control and node 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 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 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 utilize existing ecosystems. Survey and public-sector studies provide guidance on consensus choices, governance, and infrastructural requirements, arguing for consortium blockchains in national-level usage for better performance and control.

B. Strengths and Limitations

Biometric-enabled blockchain voting systems are efficient against identity threats and multiple voting, as facial recognition links ballots to unique individuals. Inclusion of deep fake detection significantly improves protection against modern attacks, strengthening the trust in biometric authentication. Nevertheless, these systems face challenges in terms of environmental sensitivity where the major drawback can be privacy concerns with biometric data, particularly if any part of the biometrics or its linkage to on-chain identities is exposed.

Hybrid/cost-optimized approaches excel in addressing the high storage and gas costs required by completely on-chain designs by storing large encrypted data off-chain(e.g. IFPS) 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 optimize transaction processing. However, these systems fail in ensuring that off-chain storage remains available, tamper-resistant, and properly synchronized with on-chain records. This method solves issues like gas price and scalability but provides us with the issue of majorly trusting the off-chain networks to maintain data and the synchronization of off-chain data with that of the on-chain.

Ethereum and smart contract–based systems offer a flexible platform for implementing voting rules, checking eligibility, and automated tallying, and they benefit from extensive tooling and a large developer community. Yet, PoW-based consensus and mainnet gas fees present huge obstacles for large-scale political elections, making such systems more suited for smaller or organizational contexts unless alternative scaling solutions are adopted. Another limitation is the dependency on cryptocurrency wallets as the primary user interface, which provides usability challenges for voters that are unfamiliar with blockchain technologies. Survey work on blockchain for e-voting further signifies the cybersecurity risks, resource intensity, and lack of advanced nationwide infrastructure - One of the main issue in India , which also resulted in the ban of cryptocurrencies in India- remain unsolved, especially when considering network conditions and device capabilities across a country.

V. Challenges

Despite promising improvements, several major 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 expensive for large-scale elections where millions of voters may cast ballots within a limited time period. In PoW voting systems, each vote needs full network verification and must wait to be added into a block. Since blocks have time and size limits, this can slow down the system and restrict how many votes it can handle at a time.

Hybrid systems offer one pathway to improved scalability by minimizing the volume of data stored on-chain, thereby reducing transaction size and associated validation. By committing only hashes of ballot results to the blockchain while holding the full encrypted data off-chain, these architectures can handle large numbers of voters without putting a lot of pressure on the consensus mechanism. However, national-scale deployment still demands strong network infrastructure, carefully analyzed block parameters, and the use of permissioned blockchains to achieve acceptable results.

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

Security in blockchain-based e-voting extends beyond ledger integrity to assure 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 using facial recognition, preventing voters from sharing credentials or being impersonated by others . However, the rise of deep fake technologies creates a new threat to this technology, where attackers might present video or images to fool face recognition systems into accepting unauthorized voters . The introduction of a deep fake detection layer is a direct solution to this threat, providing an additional classification stage that can detect manipulated media and thus prevent fraud votes, with reported high accuracy on benchmark datasets(e.g..Kaggel) .

Despite these advances, privacy remains a major concern, as biometric data is 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, other 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(private-chain 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, resulting in the need for advanced and secure governance and monitoring coupled with technical safeguards such as machine learning–based anomaly (as discussed in the Ethereum and Smart Contract–Based E-Voting Systems) detection in voting traffic and node behavior.

C. Cost, Gas Fees, and Infrastructure Requirements

Cost is a critical barrier to blockchain-based voting at a large scale, especially on public platforms that charge transaction fees. Ethereum-based voting systems demand gas fees for each transaction associated with voter authentication, vote casting, and result computation, making large-scale elections financially unfeasible on the mainnet. These costs arise due 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 reduce gas costs, such methods can reduce reliance on the public chains and may require separate governance and security.

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 lowers transaction fees and storage problems significantly. Surveys of blockchain-based e-voting state that apart from the gas costs, nation-wide voting on blockchain requires spending an extensive amount of money on network infrastructure, hardware, and biometric capture devices, particularly in regions with limited network connectivity. Therefore, while small test systems conclude that the technology can work, real national elections require a massive amount of planning and funding.

VI. Conclusion

Blockchain-based e-voting systems present a compelling vision for modernizing election 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—can be technically implemented and can address many weaknesses of traditional paper-based ,EVMs and centralized e-voting systems. In particular, biometric systems target identity theft and booth capturing, hybrid architectures work on 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 emphasize that these advances have not yet resolved fundamental challenges in terms of scalability, cybersecurity, infrastructure readiness, and regulatory integration at national scale, meaning that they are viable to be implemented on a smaller scale but have major concerns to be addressed on a larger scale. PoW-based face limitations in Capacity 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, making the ongoing work in privacy-preserving cryptography, secure off-chain storage, and advanced anomaly detection utmost necessary. Overall, while blockchain-based e-voting is supposed to significantly enhance electoral integrity and transparency, its transition from experimental prototypes to nationwide deployment hinges on addressing scalability, developing cost-effective and privacy-respecting architectures, and integrating these technical systems within 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.