WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain-Based E-Voting System

Alok Dixit[1], Mayank Jain[2], Aman Kumar[3] and Akash Kumar[4]

IIMT College of Engineering, Greater Noida
dixitalok005@gmail.com mayankjain13062005@gmail.com amankumar123bth@gmail.com akashk54130@gmail.com

ABSTRACT

This paper proposes an improved blockchain-based electronic voting framework addressing scalability, security, and issues of trust for national elections. We propose to design a permissioned consortium blockchain using a Byzantine Fault Tolerant consensus algorithm to ensure fast finality and controlled participation. To accommodate large electorates, our system employs election-specific sidechains, allowing data and computation for each election to be properly isolated from each other, with parallel operation and reduced on-chain load. Ballots are collected off-chain, and only a Merkle root commitment of the votes is stored on-chain, which enables efficient proof-of-inclusion with minimal on-chain data. Voters authenticate via their national ID and receive one-time voter tokens in such a way that only eligible citizens may vote while preserving privacy. Our design also allows for re-voting: it provides that voters can cast multiple ballots during early voting, but only their last vote is counted. This ensures "one person, one vote." Cost is optimized through cloud deployment and sidechain sharding, and its multi-stakeholder governance model ensures that no single entity is in a position to dominate the network. We elaborate on each component of the system, demonstrating how these innovations collectively enable a practical, secure, and scalable e-voting platform.

Keywords: Blockchain, Electronic Voting, Consortium Blockchain, Hybrid Blockchain**,** Coercion Resistance, Re-Voting, Off-Chain Voting**,** Merkle Commitment

1. Introduction

- Elections that are transparent and safe are essential for democracy. However, traditional paper-based voting is costly, ineffective, and prone to fraud. Blockchain provides a decentralized, tamper-proof record that allows for verification from start to finish. This feature could make it a viable option for electronic voting. Each vote can be permanently recorded on the blockchain, making it almost impossible to change without authorization. Still, public blockchain solutions face challenges related to privacy, performance, and cost. For example, the proof-of-work agreement used by open blockchains consumes unnecessary resources, and their public addresses can expose voter identities. Transaction speed and finality time are also crucial for large elections.
- Several solutions have appeared in recent studies. Off-chain protocols can reduce data on the blockchain. Sharding or sidechains can speed up transaction processing by working in parallel. Permissioned blockchains eliminate wasteful consensus and allow only trusted validators to participate. For instance, Hyperledger Fabric is a private blockchain where only verified nodes contribute to consensus. Likewise, sidechain frameworks can manage electronic votes outside the main ledger, encrypting votes on sidechains while sending only summed results to the blockchain. To increase voter confidence, researchers have examined mechanisms like one-time tokens, such as those tied to national IDs, and blind-signature tokens to maintain a balance between anonymity and verification. Additionally, countries like Estonia allow voters to cast multiple ballots during early voting, counting only the last vote from each person to minimize coercion.
- Building on these findings, we propose a practical e-voting framework that combines several innovations. This includes a consortium blockchain with Byzantine Fault Tolerance consensus, election-specific sidechains with Merkle-committed ballots, a policy that counts only the last vote, national ID-based authentication tokens, cost-efficient infrastructure, and governance involving multiple stakeholders. The remainder of this paper explains each element in detail, providing a clear blueprint for deployment.

2. Literature Survey

S.no	Paper Title	Authors	Year	Methodology
1	Blockchain for Electronic Voting System—Review and Open Research Challenges	U. Jafar, M.J.A. Aziz, Z. Shukur	2021	Conceptual review of blockchain e-voting (overview of benefits and challenges)

S.no	Paper Title	Authors	Year	Methodology
2	A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems	U. Jafar, M.J.A. Aziz, Z. Shukur, H.A. Hussain	2022	Systematic literature review (SLR) and meta-analysis on blockchain e-voting scalability (76 papers)
3	Blockchain-Based E-Voting Systems: A Technology Review	M. Hajian Berenjestanaki, H.R. Barzegar, N. El Ioini, C. Pahl	2024	Hybrid systematic review (PRISMA) of 252 papers on blockchain e-voting (analyzing benefits, challenges, architectures)
4	Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges	H.O. Ohize, A.J. Onumanyi, B.K. Nuhu, et al.	2024	Comprehensive survey of blockchain e-voting architectures, trends and solutions (overview of key aspects, performance)
5	A coercion-resistant blockchain-based E-voting protocol with receipts	C. Spadafora, R. Longo, M. Sala	2023	Cryptographic protocol design (receipt-based verification) with formal security proof for coercion-resistant voting
6	VOTEAGAIN: A scalable coercion-resistant voting system	W. Lueks, I. Querejeta-Azurmendi, C. Troncoso	2020	Design of revoting-based protocol; security proofs of privacy/coercion-resistance; prototype implementation and scalability evaluation
7	Improving Election Integrity: Blockchain and Byzantine Generals Problem Theory in Vote Systems	P. Mwansa, B. Kabaso	2024	Design science study using mixed methods (stakeholder surveys + election data simulation) to develop a blockchain vote-counting protocol
8	E-voting system using cloud-based hybrid blockchain technology	B. Jayakumari, S. Lilly Sheeba, M. Eapen, J. Anbarasi, V. Ravi, A. Suganya, M. Jawahar	2024	Design and implementation of a cloud-based hybrid blockchain e-voting system (smart contracts, PBFT consensus); performance evaluation
9	Distributed-Ledger-Based Blockchain Technology for Reliable Electronic Voting System with Statistical Analysis	R. Ch, D.J. Kumari, T.R. Gadekallu, C. Iwendi, P.K. Singh	2022	Ethereum-based e-voting dApp implementation (Ganache/MetaMask) with statistical analysis of blockchain transactions
10	Minimal Anti-Collusion Infrastructure (MACI)	V. Buterin, J. Drake, et al.	2019	On-chain voting protocol design using encrypted ballots and zk-SNARK proofs for collusion resistance (Ethereum research design)

3. Literature Review

Blockchain's decentralized ledger can strengthen e-voting by providing auditability and tamper-evidence. For example, pilots in Estonia and Switzerland demonstrate that blockchain voting can enhance security and transparencyHowever, surveys note persistent challenges: Jafar *et al*. report that blockchain systems "may help solve some of the issues that now plague election systems," yet they still suffer from shortcomings in voter privacy and transaction throughput. In general, these reviews conclude that while blockchain can remove a central authority and enable end-to-end verifiability, practical e-voting designs must still address scalability and privacy trade-offs.

To balance decentralization with practical governance, *permissioned* blockchains are often proposed for elections. In a consortium model, only pre-authorized nodes (e.g. election authorities or institutions) participate in consensus. This provides "both decentralization and control within a trusted group," ensuring all participating organizations can audit the voting ledger. For instance, Quorum-based consortium architectures have been illustrated where multiple government bodies jointly run the chain: each organization operates nodes that validate votes via smart contracts while viewing all results. Hybrid blockchain designs combine a public chain (for transparent audit trails) with a private chain (for confidential data) to leverage the strengths of both. In such systems, generic election information (e.g. tallies or bulletin-board commitments) can be posted on a public ledger, while individual vote details remain on a permissioned ledger that only authorized nodes can access. This hybrid approach seeks to obtain public trust (through a public blockchain's immutability) together with the privacy and access control of a private chain.

Another critical line of work focuses on **coercion resistance and re-voting**. Some schemes allow voters to produce decoy ballots or receipts to thwart coercion; for example, Spadafora *et al.* propose a blockchain voting protocol with cryptographic receipts that is explicitly coercion- and vote-selling-

resistant while remaining transparent. Other methods use a *revoting* paradigm: Lueks *et al.* introduce **VOTEAGAIN**, a scalable e-voting scheme where voters can override coerced votes by casting new ballots. VOTEAGAIN hides such revoting via deterministic padding (adding dummy ballots) so that an observer cannot tell if a voter re-submitted; this design achieves verifiability and coercion-resistance with only quasi-linear tallying time. These works demonstrate practical strategies for coercion-resistance in remote voting, although each has trade-offs (e.g. voter burden or complexity of dummy ballot management).

Finally, recent proposals explore **off-chain** mechanisms to improve scalability and privacy. Tang *et al.* (2023) describe an e-voting scheme where heavy cryptographic proofs are generated off-chain: voters' identity proofs (using zk-SNARKs and a Merkle tree) are computed off-chain and only verified on-chain to reduce blockchain load. Likewise, Ethereum's Minimal Anti-Collusion Infrastructure (MACI) suggests batching votes off-chain: the coordinator collects votes and publishes only a Merkle root on-chain, using a zk-SNARK to ensure the final tally reflects all committed votes. Such approaches maintain end-to-end verifiability while minimizing on-chain transactions. More broadly, reviews note that off-chain channels, sharding, and layer-2 rollups (e.g. Lightning Network style solutions) are promising for boosting throughput in blockchain voting systems.

4. Proposed System

- The proposed national e-voting system uses a permissioned consortium blockchain secured by Byzantine-fault-tolerant consensus, where state and regional data centers act as validators. Blocks are finalized only after two-thirds approval, ensuring immediate finality and preventing tampering. No raw votes or personal data are stored on-chain; only cryptographic summaries are recorded. Despite being permissioned, decentralization is maintained through multiple independent validators. Smart contracts enforce strict governance, requiring multi-party approval from the election commission, judiciary, and political parties for actions such as software upgrades or adding new nodes.
- Scalability is achieved through election-specific sidechains that operate independently and submit only aggregated results—Merkle roots and tallies—to the main chain. This parallel architecture significantly increases throughput and minimizes on-chain data usage and fees. Encrypted ballots remain off-chain, organized within a Merkle tree whose root is committed on-chain. Voters receive Merkle proofs allowing them to verify inclusion of their ballots without exposing vote content, enabling end-to-end verifiability while preserving privacy.
- The system supports re-voting during the advance period, following a "last-vote-counts" model similar to Estonia's. Each new vote invalidates the previous one, and an in-person paper vote supersedes all electronic ones. Voter eligibility is enforced through national ID authentication and issuance of blind-signed, single-use voting tokens that prevent double voting without linking identities to ballots.
- Cost efficiency is achieved through cloud-based deployment with auto-scaling and ephemeral sidechains. Governance is decentralized through a multi-stakeholder committee, with all critical actions requiring multi-signature approval and recorded immutably on-chain for transparency and auditability.

a) Advantages of the Proposed System

- **Security and Integrity:**

  The BFT consensus ensures that even if some validators misbehave, blocks cannot be forged or altered. Each block cryptographically links to the previous one, making tampering immediately detectable. Permissioned validators eliminate Sybil attacks, and blind-signature tokens prevent double-voting while keeping ballots anonymous. Once a Merkle root or tally is on-chain, it is immutable.

- **Decentralization and Transparency:**

  Validators run in distributed, independent data centers, removing single points of failure or control. All committed election data—Merkle roots, tallies, governance actions—is publicly verifiable. Smart contracts automatically enforce election rules, ensuring consistent and neutral operation. Political parties, auditors, and citizens can independently verify the election process.

- **Privacy with Verifiability:**

  No unencrypted ballots or personal identifiers appear on-chain. Blind-signed tokens ensure that identities and votes remain unlinkable. Meanwhile, Merkle proofs allow each voter to verify that their ballot was included, and auditors can recount using cryptographic data alone. This ensures end-to-end verifiability without compromising secrecy.

- **Accessibility and Convenience:**

  Remote voting enables participation from anywhere, benefiting disabled, remote, or expatriate voters. The system may still support paper voting for inclusiveness. Because voters can verify vote inclusion with cryptographic proofs, confidence in correctness can increase.

- **Cost Efficiency:**

  Digital voting removes or reduces costs for printing ballots, transporting materials, staffing polling stations, and storing physical records. Cloud infrastructure and sidechains reduce the need for permanent servers. Aggregated on-chain data minimizes blockchain transaction fees.

- **Fraud Resistance:**

One-time tokens tied to verified identities stop unauthorized voting. Distributed governance prevents insiders from controlling results unilaterally. Cryptographic protections make forging or altering votes infeasible. The tolerance of BFT consensus ensures security even if some validators are compromised.

- **Auditability and Trust:**

  Every action—vote submission, token issuance, governance change—is logged immutably. Auditors can recompute ballot totals from Merkle roots. Any discrepancy is easily detectable, enabling transparent recounts and boosting trust in results.

b) Challenges and Considerations

- **Scalability:**

  Handling millions of concurrent voters—especially during peak periods—requires robust load testing, autoscaling, and optimized network protocols. Even with sidechains, maintaining low latency and high reliability is difficult at national scale.

- **Digital Divide:**

  Citizens lacking reliable internet or digital literacy risk disenfranchisement. Assisted digital stations, mobile voting units, or hybrid paper options may be required to ensure fairness.

- **Identity vs. Anonymity Risks:**

  National ID systems introduce privacy concerns. If compromised, they may enable coercion or vote-selling. Strong legal and technical safeguards must prevent linking identities to cast ballots.

- **Endpoint Security:**

  Attacks on voter devices (malware, phishing) remain a major risk and could alter votes before encryption. Client-side verification, secure apps, and strict auditing are essential.

- **Governance Complexity:**

  Multi-stakeholder decision-making can be slow or contentious, requiring clear rules to avoid deadlocks.

- **Legal Uncertainty:**

  Many jurisdictions lack laws validating online or blockchain-based voting. Clear regulations are needed for disputes, recounts, evidence standards, and data protection.

- **User Trust and Adoption:**

  Public confidence must be built gradually through pilot programs, independent audits, transparent documentation, and education.

5. Conclusion

We have presented an **enhanced blockchain-based e-voting framework** tailored for practical deployment in national elections. By combining a permissioned consortium ledger, election-specific sidechains, off-chain Merkle-committed ballots, one-time authentication tokens, and a last-vote-counts policy, our design addresses key obstacles of security, scalability, and trust. Our analysis shows these elements working in concert to ensure vote integrity and transparency, while optimizing cost and respecting voter privacy. The proposal preserves democratic principles: only eligible voters participate, each votes once (or with re-voting safely bounded), and independent bodies oversee the process.

Future work involves prototyping and pilot testing. Performance benchmarking (e.g. with millions of virtual voters) will refine system parameters. Cryptographic protocols (such as blind signatures for tokens) must be implemented and validated. Legal and user-interface aspects will require attention to gain public acceptance.

6. Acknowledgement

The authors would like to express their sincere gratitude to the researchers and scholars whose foundational work has significantly contributed to the advancement of blockchain-based electronic voting systems. This research review has drawn extensively from a wide range of studies addressing architectural innovations, cryptographic mechanisms, and implementation strategies in the field of secure and verifiable e-voting.

In particular, we acknowledge the contributions of U. Jafar, M. Hajian Berenjestanaki, H.O. Ohize, W. Tang, C. Spadafora, W. Lueks, Vitalik Buterin, and other authors whose insights into consortium blockchains, coercion-resistance, hybrid protocols, and off-chain optimization have directly informed and strengthened the framework proposed in this paper. Their commitment to advancing secure, transparent, and scalable electoral systems continues to inspire ongoing innovation in the field.

We are grateful for their valuable research, which forms the backbone of our literature review and has guided the design of our proposed model for nationwide, trustworthy e-voting using blockchain technologies.

7. References

[1] U. Jafar, M. J. Ab Aziz, and Z. Shukur, "Blockchain for Electronic Voting System—Review and Open Research Challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021.

[2] H. O. Ohize *et al*., "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges," *Cluster Computing*, vol. 28, art. no. 132, 2025.

[3] W. Tang, W. Yang, X. Tian, and S. Yuan, "Distributed Anonymous e-Voting Method Based on Smart Contract Authentication," *Electronics*, vol. 12, no. 9, p. 1968, 2023.

[4] C. Spadafora, R. Longo, and M. Sala, "A coercion-resistant blockchain-based E-voting protocol with receipts," *Adv. Math. Commun.*, vol. 17, no. 2, pp. 500–521, 2023.

[5] W. Lueks, I. Querejeta-Azurmendi, and C. Troncoso, "VOTEAGAIN: A scalable coercion-resistant voting system," in *Proc. 29th USENIX Security Symp. (SEC)*, 2020, pp. 1553–1568.

[6] V. Buterin, "MACI with mostly-off-chain "happy path"," *Ethereum Research*, 11 May 2024.

[7] M. Hajian Berenjestanaki *et al*., "Blockchain-Based E-Voting Systems: A Technology Review," *Electronics*, vol. 13, no. 1, p. 17, 2024.

[8] M. Sharp, L. Njilla, C.-T. Huang, and T. Geng, "Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal," *Network*, vol. 4, no. 4, pp. 426–442, 2024.

[9] P. McCorry, M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "On Secure E-Voting over Blockchain," *Digital Threats: Res. Pract.*, vol. 2, 2021.