Journal of International Research & Multidisciplinary Innovation

Feasibility of Blockchain Technology in the Indian Electoral Processes: A Comprehensive Review

Tagged Discipline(s): Engineering and Technology, Humanities, Political Science

Author: Adv. Avanishkumar J. Yadav

Affiliation: Maharashtra National Law University, Mumbai

Email: avanish@lynxlegal.in

Submitted to: Journal of International Research & Multidisciplinary Innovation (JIRMI)

Date: 12 January 2026

Abstract

This paper examines the feasibility of integrating blockchain technology into the Indian electoral process, the largest democratic exercise globally. Faced with a demographic crisis of voter disenfranchisement driven by domestic migration, the Election Commission of India has actively explored remote voting technologies. Concurrently, persistent public skepticism regarding the opacity of existing Electronic Voting Machines (EVMs) necessitates a transition towards End-toEnd Verifiable (E2E-V) systems. This research employs a multi-dimensional methodology, synthesizing cryptographic literature, empirical data from regional e-voting pilot studies, and rigorous legal analyses of Indian constitutional frameworks, including the Representation of the People Act, 1951, and the Digital Personal Data Protection (DPDP) Act, 2023. The principal findings indicate that while pure internet-based public blockchains present catastrophic nationalscale cybersecurity risks and exacerbate the digital divide, a hybrid architectural convergence is highly viable. By integrating consortium blockchains with secure, localized EVM hardware and employing advanced cryptographic protocols like the Minimal Anti-Collusion Infrastructure (MACI) and Chameleon Hashing, the system can successfully reconcile absolute cryptographic immutability with coercion resistance and statutory privacy mandates. The paper concludes that this hybrid paradigm offers a pragmatic, secure, and legally compliant roadmap for the future of Indian elections.

Keywords: Blockchain voting, Electronic Voting Machines, DPDP Act 2023, End-to-End Verifiability, Minimal Anti-Collusion Infrastructure, Chameleon Hashing.

Introduction

The democratic architecture of the Republic of India represents the most massive and logistically complex electoral exercise in human history, characterized by a continuously expanding electorate that presently exceeds 900 million registered voters. The sheer magnitude of this democratic undertaking necessitates an electoral infrastructure capable of ensuring absolute integrity, extreme scalability, and uncompromising accessibility. Despite the robust logistical frameworks historically deployed by the Election Commission of India (ECI), the General Elections of 2019 witnessed a total voter turnout of 67.4%, leaving an estimated 30 crore (300 million) eligible electors completely disenfranchised.[1] Exhaustive demographic analysis reveals that a highly significant proportion of this non-participation is directly attributed to domestic migration. Driven by imperatives such as employment, higher education, and marriage, a vast segment of the Indian populace is perpetually transient, effectively severed from the geographical constituencies where their voting rights are registered.[1] To combat this systemic, migration-based disenfranchisement, the ECI has actively explored paradigm-shifting technological interventions to enable remote voting, aiming to fulfill the foundational democratic mandate that no voter is left behind.[3] The ECI's recent development of a Multi-Constituency Remote Electronic Voting Machine (RVM) prototype, capable of handling up to 72 constituencies from a single polling booth, highlights the urgency of this transition.[1]

Simultaneously, the electoral ecosystem is grappling with a brewing crisis of public trust regarding the opacity of existing voting infrastructure. In recent years, blockchain technology—a decentralized, immutable, and transparent distributed ledger system initially conceptualized for cryptocurrency transactions—has emerged as a highly debated theoretical panacea for the vulnerabilities and rigidities inherent in both traditional paper ballots and conventional electronic voting systems. Propelled by high-level discussions initiated in October 2019 by Chief Election Commissioner Sunil Arora during an institutional visit to the Indian Institute of Technology Madras (IIT Madras), a concerted exploratory effort was launched.[4] The ECI, acting in collaborative partnership with IIT Madras and the Centre for Development of Advanced Computing (CDAC), sought to engineer a secure, blockchain-enabled remote e-voting process.[5]

However, the proposed transition from India’s battle-tested, hardware-isolated Electronic Voting Machines (EVMs) equipped with Voter Verifiable Paper Audit Trails (VVPATs) to a distributed ledger framework introduces profound structural, constitutional, and cryptographic complexities. This exhaustive research paper provides a multi-dimensional, expert-level analysis of the feasibility of deploying blockchain technology across the entirety of the Indian electoral process. It scrutinizes theoretical cryptographic architectures, empirical data from regional pilot studies, evolving hybrid blockchain-hardware solutions, rigid constitutional and legal frameworks,

extreme socio-economic barriers, and the dynamic innovations being engineered to bridge the gap between digital immutability and sovereign democratic requirements.

The Demographic Crisis of Electoral Participation and the Migrant Imperative

To understand the urgent impetus behind the exploration of advanced voting technologies, one must first analyze the demographic crisis of participation within the Indian electorate. The foundational premise of a representative democracy is universal adult suffrage; however, the geographical rigidity of the current electoral system inherently discriminates against the mobile citizen. As previously established, the 2019 General Elections saw a voter turnout of 67.4%, meaning over 300 million eligible citizens failed to exercise their franchise.[1]

Data extracted from the public domain indicates that approximately 85% of internal migration in India occurs within state borders, predominantly driven by the rural population migrating outward for economic sustenance, education, and marital relocations.[1] This domestic migration acts as the primary catalyst for voter disenfranchisement. Upon assuming office, Chief Election Commissioner Rajiv Kumar highlighted this crisis following a direct, first-hand assessment of domestic migration issues during a trek to Dumak village in the Chamoli district.[1] This localized observation underscored a macro-level systemic failure: voters are routinely denied their franchise due to the sheer logistical impossibility and financial burden of traveling back to their home constituencies on polling day.[1]

To quantify the socio-political sentiment surrounding remote voting solutions, a highly focused demographic survey was conducted in September 2023 by Lokniti-CSDS.[2] The study targeted 1,017 migrants residing in the slum areas of Delhi, comprising a gender distribution of 63% men and 37% women.[2] The empirical findings laid bare the structural deficiencies of current registration systems: while 53% of these migrants had managed to register as voters in their current location of Delhi, a significant 27% remained registered in their home states, effectively neutralizing their political voice in both jurisdictions.[2] The survey also measured the intended user base's trust in proposed remote voting systems. The data revealed a deeply fragmented consensus: 47% of respondents expressed a baseline trust in the concept of a remote voting system, whereas 31% explicitly expressed distrust.[2] Furthermore, this trust metric was highly stratified by gender and education, with 50% of male respondents showing trust compared to only 40% of female respondents, and higher overall trust correlating heavily with higher educational attainment.[2]

Public Distrust, the Supreme Court, and the EVM Infrastructure

To accurately assess the feasibility of introducing blockchain voting, it is imperative to contextualize the deep-seated public skepticism regarding current EVM-VVPATs and the rigorous

judicial oversight governing technological evolution. The Indian legal system does not permit the arbitrary deployment of new electoral technologies; the transition from paper ballots to advanced digital systems is deeply intertwined with statutory definitions and legislative mandates.

The Genesis and Legal Battles of the EVM Infrastructure

The conceptualization of Electronic Voting Machines in India did not originate in the software era but was initiated in 1977, with early hardware prototypes developed by the Electronics Corporation of India Limited (ECIL).[6] By 1979, the first working models were demonstrated, and the technology was subsequently deployed on a pilot basis in May 1982 in the Parur Assembly Constituency in Kerala.[7] The ECI authorized this pilot utilizing its plenary powers derived from Article 324 of the Constitution of India.[7]

However, this technological leap faced immediate legal challenges, culminating in the landmark 1984 Supreme Court judgment of *A.C. Jose v. Sivan Pillai*.[6] The Supreme Court struck down the use of EVMs, ruling that the ECI's plenary powers under Article 324 must be read harmoniously with the Representation of the People Act (RPA), 1951, which explicitly prescribed manual ballot papers.[10] The judiciary sternly noted that the ECI cannot act as an "absolute despot" in the field of elections, completely excluding mechanical processes at that time.[12] Consequently, technological modernization was halted until the Indian Parliament amended the RPA in 1988, inserting Section 61A to legally sanction the use of "voting machines".[13]

Addressing Modern Mistrust: The 2024 Supreme Court Ruling

Despite being completely hardware-isolated—with software burned into One Time Programmable (OTP) masked chips incapable of receiving external signals—EVMs continue to face immense public scrutiny.[3] The inner workings of the EVM are perceived as a "black box," lacking the Endto-End Verifiability (E2E-V) that cryptographic systems offer.

This brewing public distrust culminated in the April-May 2024 Supreme Court hearings (Association for Democratic Reforms v. Election Commission of India) just prior to the General Elections. Petitioners sought 100% VVPAT slip verification or a return to paper ballots, citing the fundamental right of a voter to verify that their vote was recorded accurately. While the Division Bench ultimately dismissed the pleas—noting that reverting to paper ballots would undo critical electoral reforms and that EVMs successfully restrict human tampering—the court explicitly acknowledged the need to bolster public confidence. The Court mandated new technical audits, ordering that symbol loading units be sealed for 45 days post-election, and allowed candidates to request post-poll verification of the microcontroller memory. This persistent legal and public friction underscores a vital reality: future electoral technologies, including blockchain, must move beyond procedural security and provide absolute, mathematical E2E-V to satisfy an increasingly skeptical electorate.

Theoretical Foundations of Blockchain in Electoral Systems

Blockchain fundamentally seeks to resolve historical voting challenges where manipulation, opacity, and lack of trust are recurring concerns.[15] The architecture relies on several foundational pillars:

Decentralization and Cryptographic Immutability

Unlike centralized databases, a blockchain distributes voting records across numerous geographically dispersed nodes, effectively eliminating a single point of failure.[5] Each block contains validated voting transactions cryptographically bound to their predecessors using complex hash functions.[15] Any malicious attempt to alter a recorded vote changes its hash value, instantly invalidating all subsequent blocks, guaranteeing that a vote cannot be unalterably retracted or tampered with.[5]

Advanced Encryption and Coercion Resistance Innovations

A blockchain voting system operationalizes the democratic process by issuing secure digital tokens.[5] To maintain voter anonymity and transparency, the literature highlights Zero-Knowledge Proofs (ZKPs) and Fully Homomorphic Encryption (FHE), allowing computational vote tallying on ciphertexts without decrypting individual ballots.

Furthermore, to combat the critical issue of voter coercion in remote environments, researchers have developed frameworks like the Minimal Anti-Collusion Infrastructure (MACI). MACI is an open-source, on-chain voting platform specifically designed to minimize the risk of collusion and bribery. By utilizing Ethereum smart contracts alongside zk-SNARKs, MACI hides how each individual voted while publicly revealing a correct, tamper-proof final tally. This cryptographic hiding ensures receipt-freeness, making it computationally impossible for a voter to reliably prove to a briber or coercer which candidate they actually selected.

Architectural Blueprints and Academic Innovations

The theoretical mechanics of blockchain are being translated into highly sophisticated software architectures by Indian technological institutes.

The BEVM Model and Plenome Technologies

The technical realization of the proposed BEVM architecture bifurcates into an Admin Module for election configuration and a User Module for secure casting via digital wallets (like MetaMask) and Smart Contracts.[17] Within academic environments, this architecture has demonstrated remarkable stability. IIT Madras successfully deployed the "BlockVote" software for their Student General Elections.[18] Developed by Plenome Technologies—an IIT Madras-incubated deep-tech start-up founded by Prof. Prabhu Rajagopal alongside Vijayaraja Rathinasamy and Anirudh

Varna—the system utilizes a pay-per-use remote election model. Validating the scalable deployment of blockchain solutions across sensitive public systems, Plenome successfully raised Rs. 6.5 Crore in seed funding to expand their interoperable, blockchain-secured data architectures across e-governance and healthcare platforms.[18]

Empirical Evidence: The Telangana Smartphone EVoting Dry Run

While academic pilots demonstrate viability, sovereign deployment requires empirical testing. The Telangana State Election Commission (TSEC), in collaboration with CDAC, conducted a dry run of a smartphone-based e-voting solution in October 2021 within Khammam.[20] The application leveraged AI facial recognition and a Distributed Ledger Technology (DLT) database.[22]

However, the empirical results highlighted severe infrastructural deficits. Out of 14,804 citizens who attempted to register, only 3,830 successfully enrolled, with 2,128 ultimately participating in the dummy election.[21] The staggering drop-off during the initial registration phase was primarily attributed to technical glitches in linking Aadhaar cards with mobile numbers for backend verification.[21] A system that disenfranchises a massive portion of willing participants due to infrastructural bottlenecks cannot currently be scaled to 900 million voters.

The Cybersecurity Critique vs. The Convergence of Hardware and Consortium Blockchains

The global cybersecurity community has historically leveled devastating critiques against internetbased blockchain voting. The vulnerabilities of internet voting are empirically documented globally; in Estonia, the only nation relying on Internet voting for up to 25% of legally-binding national elections, independent security audits by international experts have repeatedly highlighted severe architectural vulnerabilities.[28] Seminal research from MIT further argues that applying blockchain to political voting is built on a fundamental misunderstanding of security guarantees.[23] Their thesis ("Going from bad to worse") highlights that while the ledger is secure, consumer endpoint devices (smartphones/PCs) are highly vulnerable to malware, Zero-Day exploits, and DDoS attacks.[23]

The Shift to Consortium Blockchains and Embedded Hardware Integration

However, modern research from 2024–2026 demonstrates that the technological paradigm is rapidly evolving to address these exact critiques. The industry is moving away from vulnerable, fully public, internet-reliant blockchains toward **Hybrid and Consortium Blockchains** integrated directly with physical hardware.

1. **Consortium Blockchains:** Frameworks like the proposed HAC-Bchain (Hierarchical Authoritative Consensus) utilize a consortium model where only trusted, verified nodes process the ledger. This severely limits vulnerability to external 51% attacks, and provides the transaction throughput necessary for a nationwide election.
2. **Hardware-Blockchain Convergence (Embedded Architecture):** To solve the endpoint vulnerability, recent IEEE 2025/2026 research highlights an innovative embedded system architecture for secure EVMs built on the blockchain. Instead of voting on a smartphone, voters utilize a specialized physical EVM within a supervised polling booth. This machine features a light-weight high-performance embedded controller with a cryptographic coprocessor that provides hardware-level tamper suppression. Votes are tokenized and processed on a private consortium blockchain in real-time, preserving end-to-end verifiability while embedded machine learning detects anomalies such as hardware breakdowns or unauthorized entry attempts.

This hybrid approach brilliantly bridges the gap: it maintains the coercion-resistant, physically secure environment of the traditional polling booth while leveraging the mathematical E2E-V, transparency, and immutability of the blockchain backend.

Legal and Regulatory Impasses: Reconciling Immutability with the DPDP Act

Even with advanced hybrid architectures, the implementation of blockchain voting faces formidable barriers enshrined in statutory law and evolving data privacy regulations.

Implementing a nationwide blockchain system would require profound parliamentary amendments to the RPA, 1951, to legally authorize cryptographic ledgers and digital identity tokens.[2] More pressingly, there is a fundamental structural conflict between blockchain's core feature—immutability—and India's Digital Personal Data Protection (DPDP) Act, 2023. The DPDP Act explicitly grants data principals the "Right to Erasure" (the right to be forgotten). If demographic data or digital identity tokens are permanently burned into a state-run election blockchain, the system irrevocably violates the DPDP Act. The European Union's GDPR, which heavily influenced India's data protection frameworks, similarly struggles with this exact tension.

Innovative Cryptographic Solutions: Chameleon Hashing

To dynamically solve this regulatory conflict, the cryptographic community is advancing the implementation of **Chameleon Hash Functions**. Standard blockchains use collision-resistant hashes to prevent any alteration. A Chameleon Hash, however, includes a highly secure mathematical "trapdoor". When a legally mandated erasure request is approved under the DPDP Act, an authorized entity can use the trapdoor key to generate a hash collision. This allows specific

personal data to be redacted or anonymized without altering the hash value of the block, thereby preserving the unbroken cryptographic integrity of the entire surrounding ledger. While complex to implement securely at a national scale, Chameleon Hashing represents a viable, innovative bridge between rigid blockchain immutability and modern privacy rights.

Conclusion

The exploration of blockchain technology within the Indian electoral ecosystem is transitioning from theoretical novelty to highly sophisticated, pragmatic engineering. While early concepts of fully remote, smartphone-based public blockchain voting rightly drew severe criticism from the global cybersecurity community due to catastrophic endpoint vulnerabilities and coercion risks, dismissing the technology outright ignores dynamic, cutting-edge advancements.

The palpable public distrust regarding the opacity of the current EVM-VVPAT system—as evidenced by recent Supreme Court challenges demanding greater verifiability—dictates that the Election Commission must eventually evolve toward systems offering mathematical End-to-End Verifiability (E2E-V). Pure software solutions remain vulnerable, and pure hardware solutions remain opaque. The most feasible and innovative trajectory for the Indian Electoral Process lies in the convergence of both: **Hybrid Consortium Blockchains integrated with secure, physical Embedded Hardware**.

By utilizing localized EVM hardware within supervised polling booths that interface directly with a private, highly scalable consortium ledger, the ECI can theoretically achieve the best of both paradigms: the coercion resistance and physical security of traditional voting, combined with the absolute transparency, immutability, and auditability of the blockchain. Furthermore, cutting-edge cryptographic developments like MACI and Chameleon Hashing provide a viable roadmap for maintaining compliance with the anti-collusion requirements and privacy mandates of the DPDP Act of 2023. While significant legislative amendments and massive infrastructural digital divides must still be overcome, these dynamic technological architectures demonstrate that a highly secure, transparent, and legally compliant blockchain-backed electoral process is a scientifically feasible reality for India's democratic future.

Bibilography

1. ECI ready to pilot remote voting for domestic migrants - PIB, accessed on May 27, 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1887248
2. Remote Voting for Migrants - Drishti IAS, accessed on May 27, 2026, https://www.drishtiias.com/daily-updates/daily-news-analysis/remote-voting-formigrants-2
3. Remote EVM ready to help migrants vote outside States: ECI - GS SCORE, accessed on May 27, 2026, https://iasscore.in/current-affairs/remote-evm-ready-to-helpmigrants-vote-outside-states-eci

4. Webinar Organised On Technology Aspects of Remote Voting - PIB, accessed on May 27, 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1645063
5. Election Commission of India working with IIT Madras and CDAC for a more efficient voting system - Principal Scientific Adviser, accessed on May 27, 2026, https://psa.gov.in/CMS/web/sites/default/files/psa_custom_files/Election%20Commission%20of%20India-IIT%20Madras.pdf
6. Supreme Court's Stand on EVMs and VVPATs - B&B Associates LLP, accessed on May 27, 2026, https://bnblegal.com/article/supreme-courts-stand-on-evms-andvvpats/
7. LEGAL HISTORY OF EVMs AND VVPATs - Election Commission of India, accessed on May 27, 2026, https://www.eci.gov.in/eci-backend/public/uploads/monthly_2022_11/10386732_LegalHistoryofEVMsandVVPATs_pdf.a942a6ed2e36892f92adecb5e88f6d3d
8. Sivan Pillai vs B.C. Jose on 17 December, 1984 - Indian Kanoon, accessed on May 27, 2026, https://indiankanoon.org/doc/1229406/
9. Article 324: Superintendence, direction and control of elections to be vested in an Election Commission - Constitution of India, accessed on May 27, 2026, https://www.constitutionofindia.net/articles/article-324-superintendence-directionand-control-of-elections-to-be-vested-in-an-election-commission/
10. A. C. Jose vs Sivan Pillai & Ors on 5 March, 1984 - Indian Kanoon, accessed on May 27, 2026, https://indiankanoon.org/docfragment/390634/?formInput=324&ref=static.internetfreedom.in
11. Electronic Voting Machine - INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES, accessed on May 27, 2026, https://ijlmh.com/wp-content/uploads/Electronic-Voting-Machine-ConstitutionalExamination.pdf
12. AC Jose vs Sivan Pillai & Ors on 5 March, 1984 - State Election Commission, Maharashtra, accessed on May 27, 2026, https://mahasec.maharashtra.gov.in/Upload/PDF/3%20A%20C%20Jose.pdf
13. Section 61A in The Representation of the People Act, 1951 - Indian Kanoon, accessed on May 27, 2026, https://indiankanoon.org/doc/7557203/
14. Credibility of Electronic Voting Machines- regarding. - PIB, accessed on May 27, 2026, https://www.pib.gov.in/newsite/printrelease.aspx?relid=159351
15. Democratic Innovation: Systematic Evaluation of Blockchain-Based Electronic Voting (2022–2025) - MDPI, accessed on May 27, 2026, https://www.mdpi.com/2227-7080/14/2/95
16. Blockchain Voting in the Indian Context: Potentials ... - TIJER, accessed on May 27, 2026, https://tijer.org/tijer/papers/TIJER2509087.pdf
17. (PDF) Blockchain based Electronic Voting System for Secure and Transparent Elections in India - ResearchGate, accessed on May 27, 2026,

https://www.researchgate.net/publication/397806677_Blockchain_based_Electronic_Voting_System_for_Secure_and_Transparent_Elections_in_India
18. IIT Madras-incubated Start-up Plenome raises Rs. 6.5 Crore in Seed Funding, targets Global Expansion - PIB, accessed on May 27, 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2146469
19. SGE 2024 Election Report.pdf - IIT Madras, accessed on May 27, 2026, https://web.iitm.ac.in/secc/assets/pdf/SGE%202024%20Election%20Report.pdf
20. TS develops smartphone based e-voting solution - The Hindu, accessed on May 27, 2026, https://www.thehindu.com/news/national/telangana/ts-develops-smartphonebased-e-voting-solution/article36865780.ece
21. Mock e-voting conducted - The Hindu, accessed on May 27, 2026, https://www.thehindu.com/news/national/telangana/mock-e-votingconducted/article37096968.ece
22. Emerging Technologies – Invest Telangana, accessed on May 27, 2026, https://invest.telangana.gov.in/emerging-technologies/
23. Going from bad to worse: from Internet voting to blockchain voting, accessed on May 27, 2026, https://www.dci.mit.edu/projects/going-from-bad-to-worse-frominternet-voting-to-blockchain-voting
24. Going from Bad to Worse: From Internet Voting to Blockchain Voting - Semantic Scholar, accessed on May 27, 2026, https://pdfs.semanticscholar.org/d60e/045731228b1118918cbd8cc41f2e19ac143f.pdf
25. Going from bad to worse: from Internet voting to blockchain voting | Journal of Cybersecurity, accessed on May 27, 2026, https://academic.oup.com/cybersecurity/article/7/1/tyaa025/6137886
26. Election Commission working with IIT-Madras on e-voting - The Hindu, accessed on May 27, 2026, https://www.thehindu.com/news/national/election-commissionworking-with-iit-madras-on-e-voting/article34170161.ece
27. Election Commission of India working on remote voting system - The Hindu, accessed on May 27, 2026, https://www.thehindu.com/news/national/system-toenable-electors-to-cast-votes-from-anywhere-in-the-works/article30836003.ece
28. Independent Report on E-voting in Estonia | A security analysis of Estonia's Internet voting system by international e-voting experts., accessed on May 27, 2026, https://estoniaevoting.org/
29. Security Analysis of the Estonian Internet Voting System - J. Alex Halderman, accessed on May 27, 2026, https://jhalderm.com/pub/papers/ivoting-ccs14.pdf