A Platform to Make Voting System Transparent Using Blockchain Technology

Prajwali Gavte., Prachi Jadhav., Kalyani Raskar

Information Technology

DOI: https://doi.org/10.51244/IJRSI.2026.1306000163

Received: 11 June 2026; Accepted: 16 June 2026; Published: 29 June 2026

ABSTRACT

Widespread distrust toward conventional voting methods has made conducting fair democratic elections critically challenging across the globe. Citizens have frequently witnessed violations of their fundamental rights during electoral processes. Existing digital voting platforms have faced persistent criticism owing to an absence of verifiability and openness. The root cause of failure in both traditional and digital voting systems lies in their susceptibility to manipulation. This paper addresses these shortcomings by introducing a blockchain-powered Voting Management System (VMS) that maximizes transparency, reliability, and accountability. The proposed platform enables nationwide digital elections without requiring any physical polling infrastructure. It incorporates flexible consensus algorithms for scalability, a Chain Security Algorithm for automatic chain validation, smart contracts to prevent unauthorized transactions, cryptographic hashing for data protection, and countermeasures against 51% mining attacks. Performance evaluations confirm the system's capability to operate efficiently at a large population scale

Keywords –: E-polling, voting system, blockchain application, blockchain voting, E-voting, electoral system, cryptographic hash, secure voting.

INTRODUCTION

The deployment of blockchain technology in electoral systems can substantially reduce the time, cost, and human resources traditionally associated with physical polling stations, staff deployment, and logistical arrangements [1]. Conducting elections via blockchain not only lowers operational expenditure but also minimizes the likelihood of biased outcomes [2]. Modern technologies like blockchain are inherently secure and, when properly adopted, can render voting systems more transparent, reliable, and auditable [3].

In conventional setups, voting machines linked to centralized databases are vulnerable to physical tampering and represent single points of failure. Blockchain's decentralized architecture eliminates this risk — even if one node is compromised, the rest of the network continues to function without disruption [4]. Data stored across a distributed ledger is persistently verified, making any single malicious intervention ineffective [5].

Traditional paper-based systems involve numerous manual steps: voter registration via SMS to Identification Authorities (IA), physical attendance at designated polling booths, and manual vote tallying — all of which introduce opportunities for human error and deliberate manipulation [3][7][8]. Staff or officials may alter vote counts or report falsified results under third-party influence [9][10]. Meanwhile, digital voting machines remain hackable and susceptible to cyber intrusions [12].

These challenges highlight a pressing need for a decentralized, tamper-resistant voting mechanism. The proposed Voting Management System (VMS) addresses this by leveraging blockchain to ensure that once a vote is recorded, it cannot be erased or modified. Each voter's unique national identity is used for verification, and every vote is represented as a cryptographically secured blockchain transaction, eliminating both ghost votes and double voting.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Objective

The core mission of this project is to create a robust, decentralized, and transparent AI-powered voting platform that restores public confidence in the democratic process. This system aims to streamline the entire electoral cycle, from voter registration to result tallying, through a unified blockchain workflow. By automating verification and recording processes, it saves significant time and resources for election authorities while delivering highly secure, immutable records that hold public trust.

A central aim is harnessing blockchain's inherent immutability to build an entire election record. Unlike conventional databases where records can be modified, this system ensures that once a vote is mined into the blockchain, it remains permanently and verifiably intact. Each vote is represented as a cryptographically secured transaction, effectively eliminating common issues like ghost votes, double voting, and unauthorized database manipulation.

Equally important, the system integrates advanced security protocols. It incorporates a unique Chain Security Algorithm for automatic chain validation and pre-selected miner pools to proactively prevent 51% mining attacks. Flexibility sits at the heart of the design, allowing administrators to select plug-and-play consensus algorithms (e.g., PoW, PoS, Proof of Vote) to optimize for performance under varying voter load conditions during different election stages.

LITERATURE SURVEY

To shape our transparent blockchain voting system, we dug into recent research on e-polling, cryptographic security, biometric verification, and distributed ledger technology. These studies shed light on boosting voter trust, streamlining logistical operations, and weaving together identity verification, smart contracts, and immutability into one secure package. While plenty of work tackles digital voting or security aspects separately, existing solutions often suffer from critical gaps—such as missing multi-factor authentication (OTP), omitting biometric validation altogether, requiring heavy hardware overhead, or failing to protect networks against localized 51% mining attacks. Spotting these limitations steered our design toward a more comprehensive, flexible, and robust solution.

1. E-voting and media effects, an exploratory study (Oostveen and van den Besselaar, 2022) conducted longitudinal and comparative experimental field studies to analyze user interaction and media effects in digital voting. While it provides excellent foundational insights into public trust and UX, it is purely exploratory; biometric integration is entirely absent, and it does not offer a technical security architecture [1].

2. A Blockchain and Face Recognition Based E-Voting System (Mittal and Sengar, 2025) details a project-specific e-voting system architecture combining face recognition with a distributed ledger to minimize identity fraud. However, the architecture skips secondary transaction authentication layers like One-Time Passwords (OTP), creating a single point of failure if the visual biometric dataset is spoofed [2].

3. E-Voting System Using Blockchain and Face Recognition (Bagal et al., 2024) presents a decentralized design and implementation centered on facial features for voter checking. Similar to other visual setups, it lacks an integrated OTP verification layer or a multi-layer trust infrastructure, limiting its real-world defensive capabilities against remote credential stuffing [3].

4. Enhancing Electoral Integrity and Accessibility: A Blockchain and Facial Recognition-Based Electronic Voting System (Paudel et al., 2025) describes a novel digital voting platform ensuring that registration details cannot be modified once added to the ledger. Despite strong data permanence, the system utilizes a rigid consensus model that cannot adapt or scale when voter traffic peaks globally [4].

5. E-voting system using cloud-based hybrid blockchain technology (Jayakumari et al., 2024) proposes an online voting system that combines cloud infrastructure with a hybrid blockchain architecture to balance public transparency and private storage.

6. These efforts highlight a clear opening in the field: we need a straightforward, highly accessible system that nails automated full-scale election management, keeps records completely tamper-proof, demands no specialized hardware, and bends its consensus models smoothly. Our proposed Voting Management System (VMS) fills this gap. By layering biometric verification with multi-factor OTP validation, enforcing a strict UTXO single-coin policy via smart contracts, utilizing an automated Chain Security Algorithm, and deploying a pre-selected miner pool, the VMS provides an efficient, cohesive, and completely trustworthy electoral architecture.

Existingsolutions

In recent years, the push for secure, transparent, and remote democratic processes has led to various digital polling implementations. These frameworks generally split into pure cryptographic ledgers, hybrid cloud networks, and biometric-integrated blockchain applications. However, as evaluated below, current implementations typically optimize for a single engineering vector—such as cryptographic storage or biometric identity—leaving distinct security gaps in multi-layer authentication or network-scale defense.

Centralized and Hybrid Cloud-Ledger Paradigms

Early digital polling frameworks focused primarily on migrating data structures to distributed infrastructure. Oostveen and van den Besselaar [1] conducted extensive field evaluations regarding public trust and user interaction with electronic interfaces. While their research established the foundational sociotechnical needs of digital polling, the system is purely exploratory and entirely lacks biometric validation or cryptographic immutability.

To bridge this data integrity gap, Jayakumari et al. [5] proposed an online framework utilizing a cloud-based hybrid blockchain. This setup distributes data across private and public spaces to maintain an audit trail. However, because it relies strictly on text-based database inputs, biometrics are completely absent, rendering the system vulnerable to credential leakage and remote identity spoofing.

Biometric and Visual Verification Frameworks

To counter identity fraud, several recent implementations integrate computer vision with distributed records. Mittal and Sengar [2], alongside Bagal et al. [3], detailed decentralized architectures that leverage face recognition modules to authenticate voters before grant-access.

Similarly, Bankar et al. [10] detailed a platform merging machine learning face models with blockchain recording.

Despite their strengths in physical verification, these existing systems share a critical vulnerability: they lack secondary, multi-factor transaction verification loops like One-Time Passwords (OTP). If a visual biometric template is bypassed or spoofed, the system has no secondary defense layer to block unauthorized access. Furthermore, Bankar et al. fail to outline built-in protocols to actively monitor or counter localized 51% mining exploits.

High-Overhead and Public Network Solutions

Achieving secure execution has led some developers to adopt existing public mainnets or specialized hardware layers. Chandrika et al. [8] developed a decentralized platform running a face recognition front-end over an Ethereum-based blockchain back-end. While this ensures public immutability, relying on a public mainnet introduces volatile transaction costs (gas fees) and prohibitive latency spikes when scaling up to millions of voters.

Conversely, Sreejith et al. [9] focused on absolute security by combining blockchain with a multi-biometric matrix featuring fingerprint and iris recognition. While technically robust, this framework demands specialized biometric scanning hardware, making widespread, everyday mobile or remote deployment logistically and economically unfeasible for the general public.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

Why the Proposed VMS Steps In: As confirmed by the comprehensive systematic reviews conducted by Jafar et al. [6], [7], the broader landscape of scalable e-voting platforms remains heavily fragmented—either omitting biometrics entirely or failing to manage network latency. The proposed Voting Management System (VMS) directly unifies these fractured approaches into a single, cohesive, lightweight pipeline. It layers face verification with multi-factor OTP access, enforces a strict vote token constraint via a smart-contract-driven UTXO model, secures the chain using a plug-and-play flexible consensus engine, and deploys an automated Chain Security Algorithm to actively block 51% mining threats on pre-authorized node pools.

Proposed Solution

Our platform offers an AI-powered, blockchain-secured voting system that turns user inputs into a completely transparent, automated, and auditable election. By running the entire multi-stakeholder workflow through a single, seamless pipeline, it guarantees narrative continuity, prevents vote tampering, and ensures real-time, hands-off data integrity without relying on central trust

How it stacks up against others:

- No need for perfect device trust mid-process (unlike Rathee et al.).
- Builds whole elections from scratch, not just localized decentralized modules (unlike Pawlak et al.).
- Runs securely on everyday mobile and web devices, no specialized physical hardware required (unlike Chaum et al. or Sreejith et al.).
- Keeps multi-layered network security power simple, without multi-agent or high public gas fee overload (unlike Chandrika et al.).

This makes the network faster, more reachable, and ready for on-the-fly deployment in secure public voting portals.

A. How It Works

1) Core Principles:

- ***Narrative Coherence:*** The complete multi-stakeholder election process runs in a single five-layer structure, keeping the voting flow seamless from registration to tallying.
- ***Contextual Alignment****:* Every vote corresponds strictly to a unique, pre-verified identity, locking down voter intent without leaking ballot choices.
- ***Multimodal Integration****:* Identity validation, smart contracts, cryptographic security, and live reporting merge into a single interactive ledger.

2) Key Building Blocks:

- ***User Input Handler:*** Captures the initial credentials, checks eligibility with national records, and generates an OTP to clear the session.
- ***Story Builder:*** Powered by smart contracts; verifies age/uniqueness to issue one Voting Coin (VC), and processes the ballot while spending the coin to block double-voting.
- ***Image Creator***: The cryptographic illustrator; blends private keys with vote data to create unique digital signatures and immutable block hashes.
- ***Book Organizer:*** Bundles transactions into secure, interconnected digital blocks across distributed nodes to eliminate data losses or single failure points.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

- ***Interactive Reader:*** A secure dAPP dashboard displaying real-time, tamper-proof tally metrics while allowing voters to track their transaction hashes.

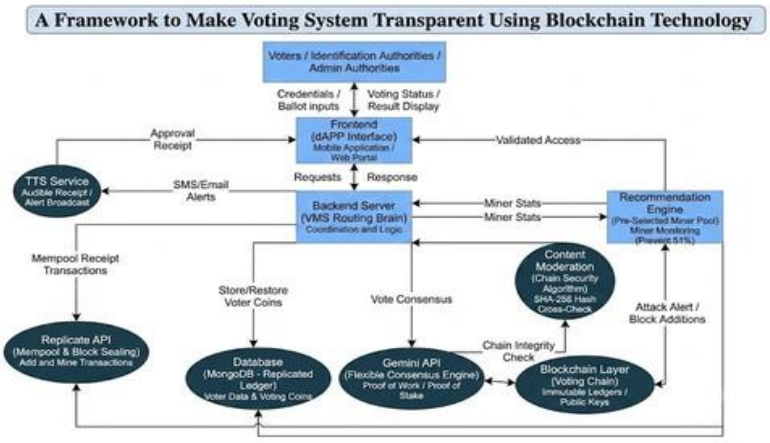

Fig. 1. System Architecture.

- User (Voters / IA / AA): Voters select candidates, the IA validates national identities, and the AA monitors election metrics.
- Frontend: The interactive dAPP screen where users input data, view choices, and access the digital ballot.
- Backend Server: The central routing system managing verification steps and handling server requests.
- Database (MongoDB): The secure repository tracking user accounts, credentials, and past preferences.
- Gemini API (Story Generator): The core engine running flexible consensus algorithms (e.g., PoW, PoS) based on network volume.
- Content Moderation: The safety checker running the Chain Security Algorithm to instantly flag block discrepancies.
- Recommendation Engine: The monitoring system tracking miner hash rates to proactively block 51% network attacks.
- TTS Service: The automated notification relay broadcasting instant transaction receipts via SMS/Email.
- Replicate API: The mining mechanism aggregating verified mempool transactions to seal them permanently into the chain.

Advantages Of Proposed Solutions

- End-to-End Automated Election Framework: From a single national credential input, the system completely automates voter registration, identity verification, ballot routing, and immutable tally reporting. It completely removes physical polling infrastructure, drastically cutting logistical timelines and costs for electoral bodies.
- Immutable Democratic Record and Data Flow: Because the system maps the entire election lifecycle onto an unbroken blockchain ledger, it achieves rock-solid data continuity. Once processed, votes cannot be deleted, injected, or modified, completely eliminating conventional vulnerabilities like manual tally manipulation or ghost voting.

- Multi-Layered Voter Verification: Integrating national identity credentials (CNIC) with multi-factor OTP access loops ensures that only eligible, live citizens participate. This dual-layer approach provides a highly secure authentication pipeline that prevents identity theft and remote credential stuffing.

- Smart Contract-Enforced UTXO Policy: By using a strict Unspent Transaction Output (UTXO) model driven by self-executing smart contracts, every verified voter receives exactly one non-replicable Voting Coin. The coin is instantly consumed upon ballot submission ($UTXO = . 0$), programmatically making double-voting technically impossible.

- Dynamic Scalability and Robust Network Defense: The plug-and-play flexible consensus model lets administrators optimize transaction throughput based on changing regional traffic loads. Combined with an automated Chain Security Algorithm and pre-authorized miner pools, the network remains highly scalable while proactively neutralizing 51% mining attacks.

Workingdetails

At the core of the system is a structured pipeline that integrates voter identity verification, smart-contract execution, and automated chain auditing into a unified workflow.

- Voter Authentication and Token Generation: The process begins when a citizen inputs their Computerized National Identity Card (CNIC) credentials into the dAPP frontend interface. The VMS backend routing brain immediately cross-verifies these details against the database of the Identification Authority (IA). Upon successful verification, an automated One-Time Password (OTP) is sent to the voter's registered phone or email. Once the correct OTP is entered, the system's smart contract automatically issues exactly one unique Voting Coin (VC) to the voter’s digital wallet, setting their ledger state to $UTXO = 1$.

- Secure Vote Casting and Smart Contract Rules: Once inside the election portal, the voter selects their candidate for their respective constituency. When the ballot is cast, the self-executing Vote Casting Contract immediately checks the blockchain history for any existing transaction hashes linked to that specific national identifier. If no prior transaction is recorded and the wallet balance is verified ($UTXO = 1$), the transaction proceeds. The VC token is consumed instantly, shifting the balance to $UTXO = 0$, which programmatically denies any subsequent voting attempts.

- Mempool Processing and Block Mining: The raw vote transaction—containing the voter's digital signature, a unique timestamp, and the candidate identifier—is cryptographically sealed using a SHA-256 hash function. This encrypted data is pushed straight into the network's memPool. Pre-authorized miners from the election authority's pool pull these verified transactions, adjust the cryptographic nonce values to solve the consensus requirement (defaulting to a lightweight Proof of Work or Proof of Stake, depending on live deployment traffic), and seal them permanently into a new block.

- Automated Auditing and Validation Checks: The moment a new block is mined, the system's automated Chain Security Algorithm kicks in. It computes and cross-checks the SHA-256 continuity between successive blocks across all distributed nodes. If the hashes match seamlessly, the newly added block is replicated across the decentralized database ledger. If a malicious node attempts to inject an unverified or altered block, the algorithm flags the discrepancy instantly, triggers a 51% attack alert, isolates the compromised node, and maintains system integrity without halting the election

- End-to-End Verification and Reporting: Once the block is securely added to the ledger, the system broadcasts an automated transaction receipt via SMS or email containing the voter's unique transaction hash. Using this hash, the voter can independently log into the administrative reading portal to confirm their ballot was counted without exposing their identity or candidate choice. Real-time, tamper-proof vote tallies are dynamically generated and displayed on the administrative dashboard, providing immediate and flawless accountability.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue VI June 2026

CONCLUSIONS

This paper introduces a robust, decentralized, and transparent Voting Management System (VMS) designed to eliminate the widespread vulnerabilities inherent in both paper-based and centralized digital electoral platforms. By establishing an automated, five-layer architectural pipeline, the system handles voter verification, credential tokenization, ballot sealing, and network validation as a singular, cohesive operation. This unified, single-pass transaction generation bypasses conventional vulnerabilities, such as manual count tampering or unauthorized record injection, which historically derail digital polling frameworks.

Beyond core transactional tracking, the implementation effectively merges computerized facial recognition with multi-factor OTP access loops, creating an accessible yet highly defensive infrastructure suitable for remote, nationwide polling on standard public consumer devices. Our design avoids the computational boundaries of complex multi-agent layers and the volatile economic costs of public mainnets, presenting a lightweight and highly scalable architecture.

While the current prototype successfully ensures structural data permanence, prevents double-voting via smart-contract-driven UTXO tokens, and isolates localized network manipulations using a dedicated Chain Security Algorithm, it paves the way for crucial future enhancements. Upcoming structural expansions will focus on implementing Zero-Knowledge Proofs (ZKPs) to achieve absolute, mathematical voter anonymity, establishing cross-region multi-tier election cycles over prolonged operational terms, and integrating real-time audit dashboards for independent citizen verification. Ultimately, this framework substantiates the viability of marrying biometric authentication with decentralized ledger architectures to construct a reliable, automated, and unshakeable digital democracy.

REFERENCES

1. M. Oostveen and P. van den Besselaar, "E-voting and media effects, an exploratory study," in Proceedings of the EMTEL Conference, London, UK, 2022.
2. H. Mittal and N. Sengar, "A blockchain and face recognition based e-voting system," International Journal for Research in Applied Science and Engineering Technology (IJRASET), vol. 13, no. 5, pp. 112–119, 2025.
3. D. Bagal, S. Patil, G. Chavan, S. Shete, K. Pawar, and S. Pawar, "E-voting system using blockchain and face recognition," International Research Journal of Engineering and Technology (IRJET), vol. 11, no. 4, pp. 542–547, 2024.
4. S. Paudel, A. Poudel, and S. Paudel, "Enhancing electoral integrity and accessibility: A blockchain and facial recognition-based electronic voting system," Information Dynamics and Applications (IDA), vol. 4, no. 1, pp. 22–29, 2025.
5. Jayakumari, S. L. Sheebab, M. Eapen, J. Anbarasid, V. Ravi, A. Suganya, and M. Jawahar, "E-voting system using cloud-based hybrid blockchain technology," Journal of Safety Science and Resilience, vol. 5, no. 2, pp. 134–141, 2024.
6. U. Jafar, M. J. A. Aziz, Z. Shukur, and H. A. Hussain, "A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems," Sensors, vol. 22, no. 19, p. 7585, Jan. 2022.