© Volume 2, Issue 10, October 2026 | JATIR
e-ISSN: 2839-5786, p-ISSN: 3139-8464

A Blockchain-Based Secure Digital Voting System with OTP and Biometric Authentication

[1]Shivani Shitole, [2]Dushyant Patil, [3]Bhojraj Patil, [4]Yashraj Sanas
[5]Shiv Kharate
[1]*Assistant Professor Information Technology Parvatibai Genba Moze College, Pune, India*
[2,3,4,5]*Student, Information Technology Parvatibai Genba Moze College, Pune, India*

***Abstract*—VoteChain is a web-based digital voting platform designed to make elections secure, transparent, and tamper-resistant by combining blockchain technology with strong voter verification. Traditional and centralized online voting systems remain vulnerable to vote tampering, identity fraud, and single points of failure, which weakens public trust in election outcomes. VoteChain addresses these problems by recording every vote as an immutable transaction on the Ethereum blockchain through Solidity smart contracts, so that once a vote is cast it cannot be altered or deleted. Voter identity is verified through a two-layer authentication process consisting of OTP verification and WebAuthn-based biometric authentication, ensuring that only registered voters can access the system and that each voter can cast only one vote. The platform provides separate dashboards for voters and administrators: administrators can add, edit, or remove candidates and monitor results in real time, while voters can register, authenticate, and cast their vote through a simple interface. Candidate-related documents can optionally be stored on IPFS for decentralized, tamper-proof access. By integrating blockchain, biometric verification, and OTP-based validation into a single system, VoteChain aims to improve the security, transparency, and efficiency of the voting process while preserving voter privacy and reducing the manual effort involved in conducting and monitoring elections.**

***Index Terms*—VoteChain, blockchain voting, Ethereum, Solidity, OTP verification, WebAuthn, biometric authentication, IPFS, digital voting, election security.**

I. INTRODUCTION

Election systems play a critical role in democratic societies by enabling citizens to cast their votes and elect representatives, and the security, transparency, and fairness of the voting process are essential for maintaining public trust. Traditional voting systems, whether paper-based or electronic, often face challenges such as vote tampering, identity fraud, lack of transparency, and delays in result processing. Online voting systems have emerged as a way to improve accessibility and efficiency, but centralized implementations remain vulnerable to cyberattacks,

data manipulation, and single points of failure, raising concerns about data integrity, voter authentication, and result transparency. Recent developments in blockchain technology, biometric authentication, and web-based security protocols provide an opportunity to build secure and decentralized voting systems: blockchain ensures immutability and transparency of vote records, while biometric authentication and OTP verification strengthen voter identity verification and prevent unauthorized access. VoteChain integrates these technologies into a single platform, combining blockchain-based vote storage with secure off-chain storage for sensitive voter data, so that the system can achieve better trust, transparency, and efficiency compared to traditional voting methods.

II. PROBLEM STATEMENT

Traditional and centralized online voting systems suffer from security vulnerabilities, identity fraud, lack of transparency, and risks of vote manipulation. Ensuring that each voter can vote only once while still preserving voter privacy remains a significant challenge for existing systems. There is a need for a secure, transparent, and reliable voting platform that provides strong voter authentication, prevents duplicate voting, and guarantees the integrity of election results from casting through to final tally.

III. MOTIVATION

The motivation behind VoteChain is to address the trust deficit created by tampering-prone and opaque voting systems. Manual and centralized digital voting processes place the burden of trust entirely on a single authority, leaving room for manipulation, disputes over results, and voter disenfranchisement through identity fraud or duplicate voting. By recording votes immutably on a blockchain and verifying every voter through OTP and biometric checks, the project aims to remove single points of failure, give voters and observers a verifiable record of the process, and reduce the administrative overhead involved in conducting secure elections.

IV. AIM AND OBJECTIVES

Aim: -
To develop a secure and transparent blockchain-based digital voting system that uses OTP and biometric authentication to verify voters and prevent duplicate voting.

Objective: -
To develop a secure and transparent digital voting system using blockchain technology.
To implement voter authentication using OTP and biometric verification for secure access.
To ensure that each voter can cast only one vote and prevent duplicate voting.
To maintain the privacy of voter information while ensuring the integrity of vote records.
To provide an efficient candidate management system for adding, editing, and removing candidates.
To enable real-time vote counting and result generation with tamper-proof storage on blockchain.

V. SCOPE OF THE PROJECT

The scope of VoteChain is to develop a secure, web-based blockchain voting platform covering the full election lifecycle. The system will cover:

- Voter Management – Registration, OTP verification, and biometric credential enrolment for each voter.
- Voter Authentication – Login using voter ID, OTP, and WebAuthn-based biometric verification.
- Candidate Management – Adding, editing, and removing candidates along with supporting documents.
- Vote Casting – One-vote-per-voter enforcement with duplicate-vote detection.
- Blockchain Vote Storage – Recording votes as smart-contract transactions on Ethereum.
- Result Dashboard – Real-time vote counting and result visualization for administrators.

VI. EXISTING SYSTEM AND ITS LIMITATION

Existing System: -

Most current elections rely on paper ballots, standalone electronic voting machines, or centralized online voting portals where a single authority controls voter records, candidate data, and vote counting.

Limitations: -

- Centralized databases create a single point of failure for tampering or data loss.
- Weak or single-factor identity checks make impersonation and proxy voting possible.
- Vote records can be altered, deleted, or disputed with no independent way to verify integrity.
- Manual or semi-manual counting delays result processing and invites human error.
- Voters and observers have no transparent way to verify that their vote was recorded correctly.
- There is no integrated, tamper-proof mechanism combining strong authentication with immutable vote storage.

VII. PROPOSED SYSTEM

VoteChain is a blockchain-based voting platform that integrates blockchain technology for secure vote recording, biometric authentication and OTP verification for voter validation, and decentralized storage mechanisms for candidate-related documents and election records. Voters register with OTP verification, enrol a biometric credential through WebAuthn, and authenticate using both factors before casting a vote. Each vote is submitted as a transaction to a Solidity smart contract deployed on Ethereum, so that once recorded it cannot be altered or deleted. Administrators manage candidates and view real-time results computed directly from the blockchain, giving the system a transparent, tamper-resistant, and efficient digital voting workflow while preserving voter privacy.

VIII. PROPOSED METHODOLOGY

The proposed system follows a modular and secure architecture consisting of the following steps:

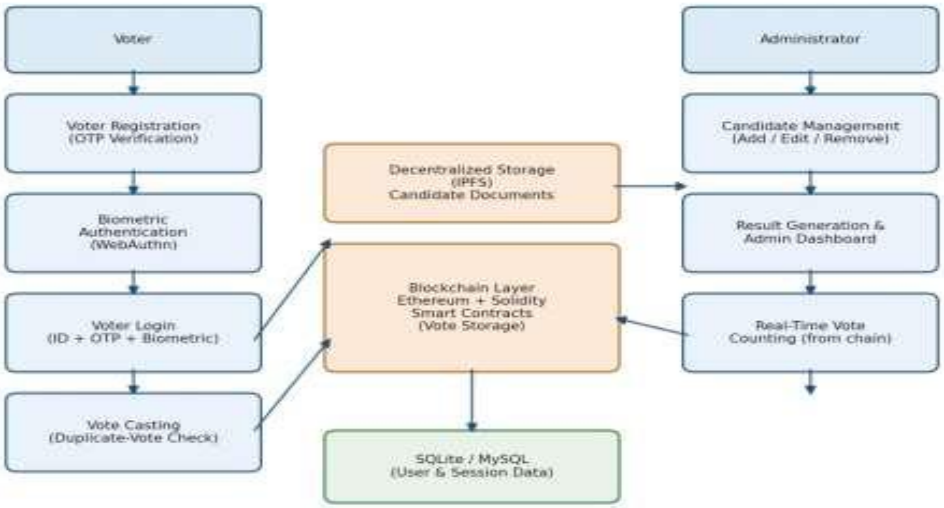
Voter Registration – Users register with personal details such as name, voter ID, email, and password, validated through OTP verification.
Biometric Authentication Registration – After registration, the voter's biometric credential is registered using WebAuthn, and the credential ID and public key are stored securely.
Candidate Management – The administrator adds, edits, or removes candidates, storing candidate name, party details, and supporting documents securely.

Voter Authentication – Before voting, the voter logs in using voter ID, OTP verification, and biometric authentication, ensuring only authorized users can proceed.
Vote Casting – The authenticated voter selects a candidate and casts a vote; the system checks whether the voter has already voted to prevent duplication.

Blockchain Vote Storage – The vote is recorded on the blockchain through a smart contract, storing only vote records and transaction proofs for transparency and immutability.

Result Generation and Dashboard – The system counts votes directly from the blockchain and displays realtime results on the admin dashboard.
User Interface Dashboard – Separate dashboards are provided for voters and administrators to manage authentication, candidates, voting, and results.

IX. SYSTEM ARCHITECTURE



X. MODULE DESCRIPTION

10.1 Voter Registration Module

This module is responsible for registering new voters in the VoteChain system. The voter provides required information such as name, voter ID, email address, and other necessary details. The system validates the submitted information and sends an OTP to the registered email or mobile number. Registration is completed only after successful OTP verification. The voter

details are stored securely in the database, while sensitive authentication information is protected from unauthorized access.

10.2 OTP Verification Module

The OTP Verification Module provides an additional layer of security during voter registration and authentication. A unique, time-limited OTP is generated and sent to the voter's registered communication channel. The system verifies the entered OTP before allowing the voter to continue. OTP records include information such as the OTP value or secure hash, creation time, expiration time, verification status, and associated voter account. Expired or previously used OTPs are rejected.

10.3 WebAuthn Biometric Authentication Module

This module provides passwordless or multi-factor authentication using the Web Authentication (WebAuthn) standard. During enrolment, the voter's device creates a public/private key pair associated with an authenticator, such as a fingerprint sensor, Face ID, Windows Hello, or another supported authenticator. The private key remains protected by the user's device, while the corresponding public key and credential identifier are stored by the application. During login, the system verifies a cryptographic authentication response instead of receiving or storing the biometric data itself.

10.4 Voter Authentication Module

The Voter Authentication Module verifies the identity of a registered voter before allowing access to the voting interface. The voter provides the required login information, completes OTP verification, and performs WebAuthn authentication. The system validates all required authentication factors before creating an authenticated voting session. This module helps prevent unauthorized users from accessing another voter's account.

10.5 Admin Authentication Module

This module provides secure access to the administrator dashboard. Only authorized administrators can access election-management functions. Administrator authentication can use strong credentials and, where required, additional authentication mechanisms. Role-based access control ensures that ordinary voters cannot access administrative operations such as candidate management or election configuration.

10.6 Candidate Management Module

The Candidate Management Module allows administrators to manage candidates participating in an election. Administrators can add candidate information such as candidate name, party or organization, description, photograph, and supporting documents. Existing candidate information can be updated or removed according to the election rules. Candidate documents may optionally be stored using IPFS, with their content identifiers maintained by the application.

10.7 Election Management Module

This module manages the lifecycle of an election. Administrators can create an election, define its basic information, configure candidates, and control the election status. The system can maintain states such as upcoming, active, and completed. Voting is permitted only when the

election is active, helping prevent votes from being submitted outside the configured election period.

10.8 Vote Casting Module

The Vote Casting Module provides the interface through which an authenticated voter selects a candidate and submits a vote. Before submission, the system verifies that the voter is eligible and has not already voted. After confirmation, the vote is submitted to the blockchain smart contract through the configured blockchain interaction layer. The application records the resulting transaction reference for later verification and auditing.

10.9 Blockchain and Smart Contract Module

This is the core integrity module of VoteChain. A Solidity smart contract deployed on the Ethereum network manages voting-related blockchain operations. The smart contract can maintain election and candidate identifiers, record voting transactions, enforce one-vote-per-voter rules according to the system design, and provide vote-counting information. Once a transaction is confirmed on the blockchain, the corresponding blockchain record cannot normally be modified through the application.

10.10 Result and Dashboard Module

The Result Module retrieves voting information from the blockchain and calculates or displays candidate vote counts. Administrators can view election statistics through a dashboard, while access to voter-facing results can be controlled according to election requirements. Blockchain transaction references provide an auditable record of vote submissions.

10.11 Database and Storage Module

The database stores off-chain application information such as voter profiles, candidate information, election configuration, OTP records, WebAuthn credential metadata, user roles, and blockchain transaction references. MySQL or SQLite can be used depending on the deployment requirements. Sensitive voter information is kept off-chain rather than being written directly to the public blockchain.

10.12 IPFS Document Storage Module

The optional IPFS module provides decentralized storage for candidate-related documents and other nonsensitive election materials. Instead of relying exclusively on a centralized file server, files can be uploaded to IPFS and identified using content-addressed identifiers. The resulting CID can be stored in the application's database or associated with candidate information.

10.13 Notification and Audit Module

This module handles system notifications such as OTP delivery, registration confirmation, authentication status, and voting confirmation. It can also maintain application-level audit information such as login events, administrative actions, and blockchain transaction references. Audit information supports monitoring and troubleshooting without exposing sensitive voter information.

10.14 User Interface Module

The User Interface Module provides separate interfaces for voters and administrators. Voters can register, authenticate, view eligible elections, select candidates, and submit their votes.

Administrators can manage elections and candidates and monitor results. The interface is designed using Next.js, Tailwind CSS, and daisyUI to provide a responsive and user-friendly experience.

XI. HARDWARE AND SOFTWARE

Hardware: -
• Processor: Intel Core i5 or equivalent.
• RAM: Minimum 8 GB.
• Storage: Minimum 256 GB SSD.
• Internet: Required for blockchain network and API-based features.
• Display: Standard monitor/laptop display.

Software: -
• Operating System: Windows 10/11.
• Programming Language: TypeScript / JavaScript.
• Frontend Framework: Next.js.
• Backend Framework: Node.js.
• Blockchain Platform: Ethereum.
• Smart Contract Development: Solidity.
• Blockchain Development Framework: Hardhat.
• Wallet Integration: MetaMask.
• Authentication: OTP Verification, WebAuthn Biometric Authentication.
• Database/Storage: SQLite / MySQL.
• Decentralized Storage (Optional): IPFS.
• UI Styling: Tailwind CSS, daisyUI.
• Biometric Libraries: SimpleWebAuthn.
• Version Control: Git, GitHub.

XII. DATABASE/UML DESIGN

The system will use MySQL/SQLite to store voter, candidate, election, and authentication details, while vote records are stored immutably on the Ethereum blockchain. UML diagrams such as Use Case Diagram, Class Diagram, and Sequence Diagram will represent the interaction and workflow of the system.
Main Database Entities:
Voter, Admin, Candidate, Election, OTP Record, Biometric Credential, Vote Transaction Reference.

XIII. INNOVATION/NOVELTY

• Combines blockchain-based immutable vote storage with a two-factor OTP and biometric authentication layer.
• Uses WebAuthn biometric credentials instead of passwords alone, reducing impersonation and proxy voting.

• Optional IPFS-based decentralized storage for candidate documents, avoiding single points of failure.
• Unified platform integrating voter management, candidate management, voting, and real-time results in one system.

XIV. EXPECTED OUTCOMES

• Secure and transparent digital voting process using blockchain technology.
• Strong voter authentication using OTP and biometric verification.
• Prevention of duplicate voting and unauthorized access.
• Tamper-proof storage of vote records ensuring data integrity.
• Real-time vote counting and accurate result generation.
• Improved trust, privacy, and reliability in the election process.
• Efficient candidate management and simplified election administration.
• Enhanced accessibility and reduced manual effort in conducting elections.

XV. APPLICATIONS

• Government and Public Elections – For secure, verifiable large-scale voting.
• Educational Institutions – For student council and college election voting.
• Corporate Governance – For shareholder voting and board elections.
• Organizations and Societies – For committee and office-bearer elections.
• Referendums and Polls – For transparent public opinion collection.

XVI. ADVANTAGES AND LIMITATIONS

Advantages
• Automates and secures vote recording using blockchain immutability.
• Two-factor OTP and biometric verification strengthen voter identity checks.
• Prevents duplicate voting through on-chain verification.
• Provides real-time, tamper-proof result generation.
• Reduces manual effort in candidate and election administration.

Limitations
• Blockchain transaction costs and network congestion can affect performance at large scale.
• Biometric accuracy may be affected by device quality or enrolment issues.
• Requires reliable internet connectivity for blockchain and OTP-based features.
• Initial voter registration and biometric enrolment require time and infrastructure.
• Regulatory and legal acceptance of blockchain-based voting varies by region.

XVII. FUTURE SCOPE

• Integration with mobile applications for voter registration and voting.
• Adoption of Layer-2 scaling or zero-knowledge proofs for improved privacy and lower cost.
• Integration with government identity systems for large-scale deployment.
• Multi-language and accessibility support for wider voter reach.

• Cloud deployment for scalable, remote election monitoring.

XVIII. LITERATURE SURVEY

Blockchain-based electronic voting has received significant attention because of its potential to provide tamper-evident records, decentralized verification, and automated election processes. However, research also identifies important challenges involving voter privacy, authentication, scalability, usability, and regulatory acceptance.

19.1 Blockchain for Securing Electronic Voting Systems

A survey of blockchain-based electronic voting systems examined different architectures, technologies, trends, solutions, and challenges. The study discusses how blockchain can improve the integrity and auditability of electronic voting by distributing transaction records across a decentralized network. At the same time, it identifies challenges such as scalability, privacy, computational requirements, and practical deployment. This work provides a foundation for the blockchain component of VoteChain.

19.2 Blockchain-Based E-Voting Systems: Privacy, Integrity and Scalability

The systematic literature review examines blockchain-based electronic voting research with particular emphasis on privacy, integrity, and scalability. The study highlights that blockchain can provide strong integrity guarantees, but simply placing voting information on a public blockchain does not automatically provide voter privacy. This observation is relevant to VoteChain because sensitive voter information is intended to remain off-chain while blockchain transactions are used for vote-record integrity.

19.3 Digital Authentication for Blockchain-Based E-Voting

The systematic review investigates authentication mechanisms used in blockchain-based electronic voting systems. It emphasizes the importance of reliable voter authentication in preventing unauthorized access and duplicate voting. The review supports the use of stronger authentication mechanisms rather than relying only on conventional passwords. VoteChain extends this concept by combining OTP verification with WebAuthn-based authentication.

19.4 Ethereum and Smart Contracts

Buterin introduced Ethereum as a platform for decentralized applications and smart contracts. Smart contracts allow application rules to be executed through blockchain transactions without requiring a centralized application server to perform every operation. VoteChain uses Solidity smart contracts on Ethereum to implement voting-related blockchain operations.

19.5 Ethereum Transaction Ledger

Wood described the technical architecture of Ethereum in the Ethereum Yellow Paper. The work explains the Ethereum transaction and state model that forms the technical foundation for decentralized applications. Understanding Ethereum's transaction model is important for designing the VoteChain smart contract and blockchain interaction layer.

19.6 Web Authentication and Public-Key Credentials

The W3C Web Authentication specification defines WebAuthn as a web API for creating and using public-key credentials. Unlike systems that require an application to store biometric

information, WebAuthn enables authentication using credentials protected by an authenticator. This technology is particularly relevant to VoteChain because biometric or device-based authentication can be performed while the application stores credential metadata and public keys rather than raw biometric information.

19.7 IPFS and Decentralized Storage

Benet introduced the InterPlanetary File System (IPFS), a distributed peer-to-peer system based on content addressing. IPFS can be used to identify and retrieve files based on their content rather than relying exclusively on a centralized file location. VoteChain can use IPFS as an optional storage mechanism for candidate documents and other non-sensitive election materials.

19.8 Bitcoin and Blockchain Technology

Nakamoto introduced Bitcoin as a peer-to-peer electronic cash system based on a distributed ledger. Although Bitcoin was designed for digital currency rather than voting, its underlying concepts of distributed consensus, cryptographic verification, and tamper-evident transaction history influenced later blockchain applications, including decentralized voting systems.

19.9 Hardhat Development Environment

Hardhat provides a development environment for Ethereum-based smart contracts. It supports contract compilation, testing, deployment, and development workflows. VoteChain can use Hardhat to develop and test the Solidity voting contract before deployment to an Ethereum-compatible network.

19.10 MetaMask and Blockchain Interaction

MetaMask provides a wallet and browser-based interface for interacting with Ethereum-compatible decentralized applications. In VoteChain, MetaMask can be used as one possible mechanism for connecting the web application to the blockchain and submitting blockchain transactions.

19.11 Overall Research Gap

The reviewed literature demonstrates that blockchain can strengthen the integrity and auditability of electronic voting, while WebAuthn and other authentication mechanisms can strengthen voter identity verification. However, important challenges remain in combining these technologies while maintaining voter privacy, usability, scalability, and secure separation between identity information and vote information. VoteChain addresses this integration at the prototype level by combining OTP verification, WebAuthn authentication, off-chain voter information, blockchain-based vote recording, and optional IPFS document storage within one web-based platform.

REFERENCE

[1]. H. O. Ohize, A. J. Onumanyi, B. U. Umar, et al., “Blockchain for Securing Electronic Voting Systems: A Survey of Architectures, Trends, Solutions, and Challenges,” Cluster Computing, vol. 28, pp. 132–170, 2025.
[2]. “Blockchain-Based E-Voting Systems: A Systematic Literature Review on Privacy, Integrity, and Scalability,” TechRxiv, 2025.

[3]. "A Systematic Review of Digital Authentication for Blockchain-Based E-Voting Systems," Iraqi Journal of Intelligent Computing and Informatics, 2025.
[4]. V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2014.
[5]. G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.
[6]. World Wide Web Consortium (W3C), "Web Authentication: An API for Accessing Public Key Credentials," W3C Recommendation, 2019.
[7]. J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," arXiv preprint arXiv:1407.3561, 2014.
[8]. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[9]. Nomic Foundation, "Hardhat Documentation: Ethereum Development Environment," 2025.
[10]. Consensys, "MetaMask Documentation: Crypto Wallet and Blockchain Applications," 2025.
[11]. T. Bray, "The JavaScript Object Notation (JSON) Data Interchange Format," RFC 8259 (IETF), 2017.
[12]. Tailwind Labs, "Tailwind CSS Documentation: Utility-First CSS Framework," 2025.
[13]. Vercel, "Next.js Documentation: The React Framework for Production," 2025.
[14]. OpenJS Foundation, "Node.js Documentation: Node.js JavaScript Runtime Environment," 2025.
[15]. SimpleWebAuthn, "SimpleWebAuthn Documentation: WebAuthn Server and Browser Libraries," 2025.