e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

Online Voting System Using Blockchain: A Comprehensive Approach

Harsh Minde[*1], Atharva Birje[*2], Ameya Mane[*3], Jyotiraditya Patil[*4], Prof. Dnyaneshwar Thombre[*5]

[*1,2,3,4]Student, Department of Computer Engineering, Terna Engineering College, Navi Mumbai, Maharashtra, India

[*5]Professor, Department of Computer Engineering, Terna Engineering College, Navi Mumbai, Maharashtra, India

ABSTRACT

This research paper presents "VoteChain", a blockchain-integrated, cross-platform mobile voting application designed to overcome the inefficiencies, security vulnerabilities, and exorbitant operational costs of traditional electoral systems in populous democracies such as India. VoteChain utilizes a hybrid architecture that leverages blockchain exclusively for immutable vote recording via smart contract while delegating non-critical operations to a secondary database, all while maintaining scalability. VoteChain enforces jurisdictionally constrained voting through region-based validation, multifactor authentication, and anti-double-voting protocols. Its robust security framework employs cryptographic hashing of voter identities, role-based access control, and automated measures to prevent cross-constituency fraud. A hierarchical UI/UX design enables voters to navigate elections by constituency, party, or region, with real-time results visualized through dynamic charts and detailed metadata analytics on demographic trends and voter turnout. Overall, VoteChain establishes a blueprint for secure, transparent, and cost-effective digital democracy, bridging the gap between decentralized trust and real-world electoral pragmatism.

Keywords: Blockchain, Smart Contracts, Hybrid Architecture, E-Voting, Voting Protocols, Security & Transparency, Digital Democracy, Mobile Voting, Cross-Platform Application.

I. INTRODUCTION

In a democratic society, the integrity of electoral processes is paramount for ensuring that the collective will of citizens is accurately reflected in governmental decisions. In India—the world's largest democracy—the challenges of conducting free, fair, and transparent elections are magnified by its immense population and diverse regional dynamics. Traditional electoral systems require colossal logistical coordination, significant financial expenditure, and extensive human resources. For instance, national elections such as the Lok Sabha polls (year 2024) incur astronomical costs, with total expenditures in recent cycles estimated to approach ₹1.35 lakh crores. These expenses cover direct government spending on infrastructure, security, administrative logistics, and the procurement and maintenance of millions of Electronic Voting Machines (EVMs), in addition to setting up nearly one million polling stations and mobilizing over 10 lakh security personnel. Despite these investments, inefficiencies remain, including disenfranchisement of migrant workers and citizens unable to vote in their registered constituencies.

Amid these systemic challenges, blockchain technology has emerged as a promising solution due to its decentralized nature, immutability, and robust cryptographic security. Its inherent tamper-proof characteristics ensure that once a vote is cast, it remains unaltered, thereby providing a level of transparency and verifiability that traditional systems struggle to achieve. However, many existing blockchain-based voting systems have been criticized for their high operational costs and inefficiencies, often stemming from redundant on-chain operations that lead to prohibitive gas fees and latency issues. Industry analyses indicate that approximately 60–70% of current blockchain e-voting prototypes face such challenges, underscoring the need for a more balanced and cost-effective approach.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

This research paper presents VoteChain, a novel, cross-platform mobile application that leverages blockchain technology exclusively for vote recording and tallying while delegating non-critical operations to off-chain solutions. VoteChain's architecture is designed to address key limitations by integrating a minimalist on-chain component—implemented through smart contracts on the Ethereum Sepolia testnet (accessed via QuickNode endpoints)—with a robust off-chain backend powered by Firebase (as a secondary database). This hybrid architecture minimizes the blockchain load, thereby reducing gas fees by an estimated 40–60%, while still ensuring the integrity and transparency of the vote count.

VoteChain is developed using Flutter, which provides an intuitive user interface and seamless interaction for voters, candidates, party heads and election officials. The system is engineered to support multiple election types—ranging from local (e.g., Gram Panchayat) to state (e.g., Vidhan Sabha) and national (e.g., Lok Sabha) elections—by dynamically managing election hierarchies and participant roles through Firebase. Multifactor authentication is employed to ensure that only eligible voters can participate, and additional off-chain measures are in place to prevent duplicate voting and unauthorized access.

By eliminating the need for extensive physical infrastructure and traditional EVMs, VoteChain aims to drastically reduce the operational costs and manpower required for elections. Moreover, the application incorporates advanced features such as detailed real-time result visualization—through both list-based and graphical formats—and comprehensive data logging for post-election analysis. Notably, once an election is concluded, non-critical vote data is archived off-chain after preserving essential logs and metadata, and a new smart contract instance can be deployed for subsequent elections. This strategy minimizes on-chain storage requirements and enhances long-term data security without compromising auditability or transparency. Additionally, if the underlying root storage is reset or cleared, the blockchain network's capacity can be efficiently repurposed for future elections, ensuring optimal utilization of resources.

This research paper details the design, development, and evaluation of VoteChain. It discusses how the system integrates blockchain technology with a secondary database to achieve scalability, cost efficiency, and high security, and it outlines the potential of such an approach to transform electoral processes in India and other democracies. Through a comprehensive analysis of VoteChain's architecture, functionality, and performance, this work positions the system as a scalable and practical solution for modernizing elections, ensuring that democratic ideals intersect effectively with technological innovation.

II. RELATED WORK

Blockchain technology offers a secure and transparent platform for digital voting by leveraging advanced cryptography and decentralized authentication. Despite its promise, challenges like scalability and user accessibility remain. This section reviews key research contributions and explores potential improvements in blockchain-enabled voting systems.

The Blockchain Enabled Online-Voting System developed by Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerjee, and Madhuri Chavan (2020) utilizes blockchain to create an immutable and transparent voting system. The project incorporates 128-bit AES encryption and SHA-256 to enhance security, ensuring that the votes cast are secure and tamper-proof. The system employs authentication methods such as unique identification keys and biometric fingerprint verification, ensuring that only authorized voters can participate. Votes are cast and recorded as blockchain transactions, preserving their integrity and transparency throughout the election process. [1]

In their paper A Privacy-Preserving Voting Protocol on Blockchain, Wenbin Zhang et al. (2018) introduced a decentralized voting protocol leveraging homomorphic encryption and distributed tallying, effectively removing the need for trusted third parties. The protocol ensures voter privacy by encrypting votes and distributing ballots across peers while also detecting and correcting dishonest votes without compromising anonymity. The system uses Hyperledger Fabric, making it particularly suitable for small to medium-scale elections where privacy is a critical concern. [2]

The paper by Stephan Neumann, Oksana Kulyk, and Melanie Volkamer (2014) describes a Usable Android Application Implementing Distributed Cryptography for Election Authorities. This Android app is designed to facilitate secure distributed key generation and verifiable vote decryption for non-technical election authorities. While it simplifies the voting process for non experts, the authors highlight that users struggled with understanding complex security concepts, suggesting the need for improved educational tools to assist users in navigating cryptographic security. [3]

Jae-Geun Song, Sung-Jun Moon, and Ju-Wook Jang (2021) developed A Scalable Implementation of Anonymous Voting over Ethereum Blockchain to address scalability issues in blockchain voting systems. Their implementation successfully scales to accommodate a larger number of voters and candidates compared to previous models, reducing time complexity and making blockchain-based voting systems more efficient and suitable for large-scale elections. [4]

The study by Yulia Bardinova et al. (2018) focused on the impact of blockchain algorithms on mobile devices with their paper Measurements of Mobile Blockchain Execution Impact on Smartphone Battery. The research found that Proof of Work (PoW) algorithms significantly increase battery discharge rates and device temperature, while Proof of Authority (PoA) algorithms have minimal impact on battery performance. Additionally, cellular connections were found to worsen battery discharge rates compared to Wi-Fi, providing essential insights into optimizing blockchain applications for mobile platforms. [5]

In Decentralized Voting Platform Based on Ethereum Blockchain, David Khoury et al. (2020) developed a decentralized voting platform where smart contracts enforce transparency and voting rules, allowing one vote per registered mobile number. The system also achieves voter authentication without relying on a third-party server, enhancing both privacy and security. This approach ensures transparency while maintaining the integrity of the election process by preventing unauthorized access. [6]

In the paper Secure Electronic Voting System using Blockchain Technology by D. Dwijesh Kumar, D. V. Chandini, and Dinesh Reddy (2020), the authors propose a system that enhances privacy by storing voter information and votes on two separate blockchains. This ensures the security of sensitive voter data while maintaining transparency. The system uses blockchain transactions for casting votes, with two-step verification via a PIN. Additionally, users can verify that their vote has been correctly recorded. The use of SHA-256 encryption ensures the immutability and security of the voting process. [7]

In Implementation of Decentralized Blockchain E-voting, Saad Moin Khan et al. (2018) propose a decentralized e-voting system that leverages blockchain to create a tamper-proof and transparent voting process. The study demonstrates how smart contracts can automate the voting process to secure vote casting, while real-time vote verification builds voter trust. The integration of a user interface via Metamask further simplifies voter interaction, making the system both accessible and secure. However, the authors acknowledge several limitations, including scalability challenges, dependency on continuous internet connectivity, a complex setup process, and the inherent requirement for Ether. They suggest that these issues can be mitigated through system optimizations such as adding offline capabilities, streamlining the setup, and exploring alternatives to traditional cryptocurrency models. [8]

In E-Voting System in Smart Phone Using Mobile Application, Kalaiyarasi et al. (2020) present an Android-based e-voting solution that employs AES256 encryption for the secure storage of votes and utilizes Firebase for OTP generation to authenticate voters. This approach facilitates remote voting, thereby reducing the risk of fraud and minimizing human errors associated with manual vote counting. The system's ability to publish results immediately after the election further underscores its operational efficiency. Nevertheless, the study highlights certain limitations, such as the lack of offline voting support—which may restrict access in remote areas—vulnerability due to reliance on OTP-based authentication, and potential security concerns arising from the use of third-party services like Firebase. [9]

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

In Survey on Blockchain Based Data Storage Security for Android Mobile Applications, Hussam Saeed Musa et al. (2019) investigate how blockchain technology can enhance the security and reliability of data storage within mobile applications. Their proposed BSADS framework, which comprises six comprehensive layers, emphasizes blockchain's advantages over traditional encryption methods by ensuring robust data integrity and auditability. The study also explores innovative solutions to address challenges related to scalability, performance, and cost, including blockchain pruning and the adoption of energy-efficient consensus algorithms, as well as the use of lightweight nodes tailored for mobile environments. Despite these promising approaches, the authors point out significant limitations such as prior unsuccessful implementations in mobile voting projects, scalability issues with platforms like Ethereum Name Service (ENS), privacy concerns due to blockchain transparency, high data storage costs, and the resource-intensive nature of smart contracts that may hinder overall performance. [10]

It shows that blockchain-enabled voting systems offer promising security and transparency enhancements for digital elections. However, challenges—ranging from scalability and energy efficiency to user accessibility and connectivity—remain. These gaps underscore the need for further research to refine and optimize blockchain-based solutions for practical, large-scale electoral applications.

III. METHODOLOGY

This section presents the systematic approach and conceptual framework for VoteChain—a blockchain-based online voting system engineered for secure, transparent, and scalable elections. The methodology is organized into three primary components: the proposed system, requirements analysis, and technology selection. Together, these elements demonstrate how VoteChain addresses modern electoral challenges while optimizing cost, performance, and security.

A. Proposed System

VoteChain's conceptual design is adapted from the Blockchain-based Secure Android Data Storage (BSADS) framework—a six-layer model originally developed for secure Android applications with blockchain-backed data storage. Although BSADS is not the final production architecture, it provides a robust blueprint for a hybrid on-chain/off-chain voting system that leverages blockchain for critical vote recording and tallying while managing non-sensitive operations off-chain. This approach minimizes transaction fees, reduces network congestion, and enhances scalability (see Fig. 1).

A.1 Technical Design

VoteChain's technical design employs the six-layer BSADS framework to balance operational efficiency with robust security. The layers are as follows:

- **User Interface (UI) Layer:** Provides the primary interaction point for all stakeholders (voters, candidates, party heads, election officers, etc.) via an intuitive, multi-screen Flutter application. It supports user registration, multi-factor authentication (MFA), vote casting, and real-time result visualization.
- **Application Logic Layer:** Manages core business workflows by validating user inputs, processing transactions, and ensuring secure communication between the UI, blockchain, and off-chain databases. It protects data in transit through encrypted channels.
- **Identity Management Layer:** Implements decentralized identity (DID) creation, cryptographic key management, and MFA. This layer verifies voter identities, enforces role-based access controls, and prevents double voting while preserving anonymity.
- **Blockchain Interface Layer:** Acts as a gateway to Ethereum (using the Sepolia testnet) for vote submissions and data queries. Libraries such as Web3dart.dart abstract the complexities of interacting with the decentralized network.
- **Blockchain Network Layer:** Utilizes Ethereum's Proof-of-Stake consensus on the Sepolia testnet to immutably record and tally votes. Connectivity services like QuickNode ensure low-latency and reliable transaction processing.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

- **Data Storage Layer:** Separates critical and non-critical data storage by recording votes and final tallies on-chain, while maintaining metadata (e.g., user profiles, logs, candidate lists) off-chain in databases like Firebase(Secondary Database). This separation reduces on-chain storage costs and optimizes overall performance.

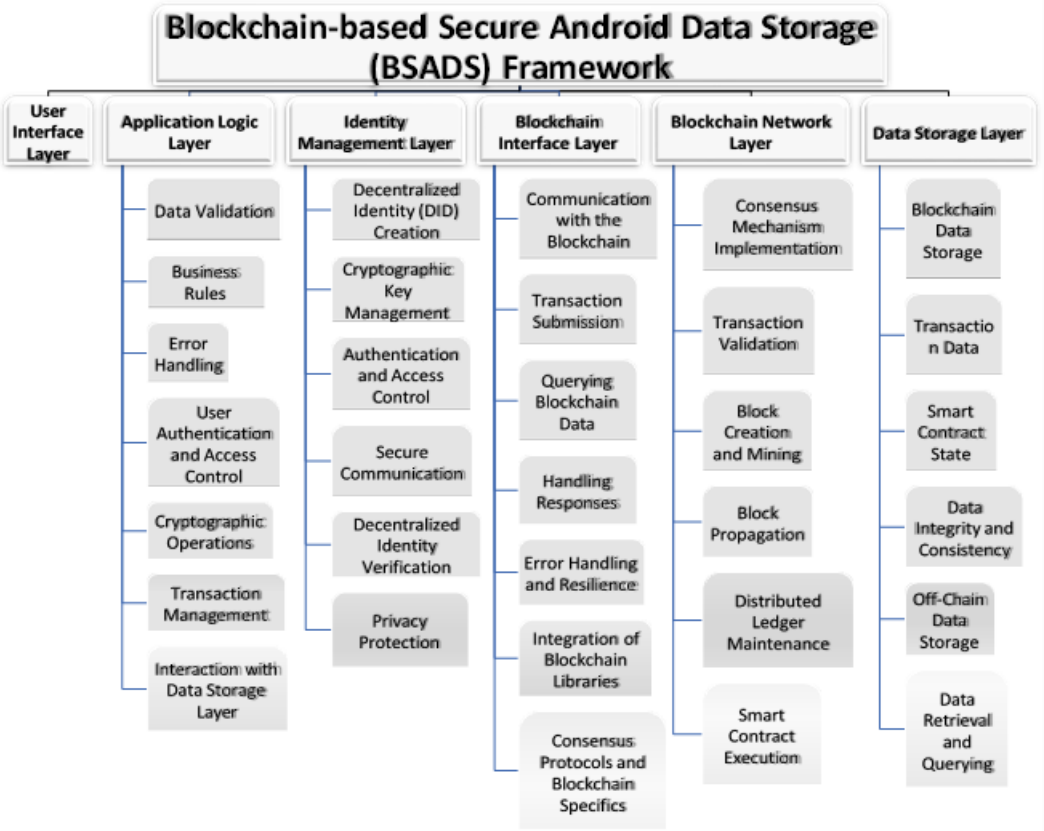

Figure 1: Proposed Framework: Blockchain-Based Secure Android Data Storage (BSADS)

Scalability and Security:

VoteChain achieves robust security through immutable vote recording and efficient off-chain management. By processing ancillary functions (such as user authentication, candidate/party management, election scheduling, and dynamic result visualization) off-chain, the system minimizes network load and gas fees. Enhanced protection is provided through MFA, end-to-end encryption, and rigorous access controls.

A.2 System Architecture and Data Flow

The hybrid architecture of VoteChain is illustrated in Fig. 2 and comprises the following core components:

- **Mobile App (Flutter):** Offers a responsive and user-friendly interface for registration, MFA login, vote casting, candidate selection, and real-time result updates (including dynamic graphical visualizations).
- **Backend System (Firebase + Web3dart.dart + QuickNode API):** Handles API requests, input validation, and secure transaction processing. It serves as the communication bridge between the mobile app, the Ethereum network, and off-chain databases.
- **Smart Contracts (Solidity):** Deployed on Ethereum Sepolia, these contracts handle vote recording and tallying. They enforce critical voting logic (e.g., verifying constituency eligibility) while minimizing on-chain operations to reduce gas costs.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

- **Blockchain Network (Ethereum Sepolia):** Provides an immutable ledger via a Proof-of-Stake consensus mechanism. Services like QuickNode support rapid, cost-effective connectivity and low network congestion.
- **Off-Chain Database (Firebase):** Manages non-critical data such as voter profiles, election metadata, candidate details, and logs. It offers real-time data synchronization and enforces role-based access control, ensuring efficient off-chain operations.

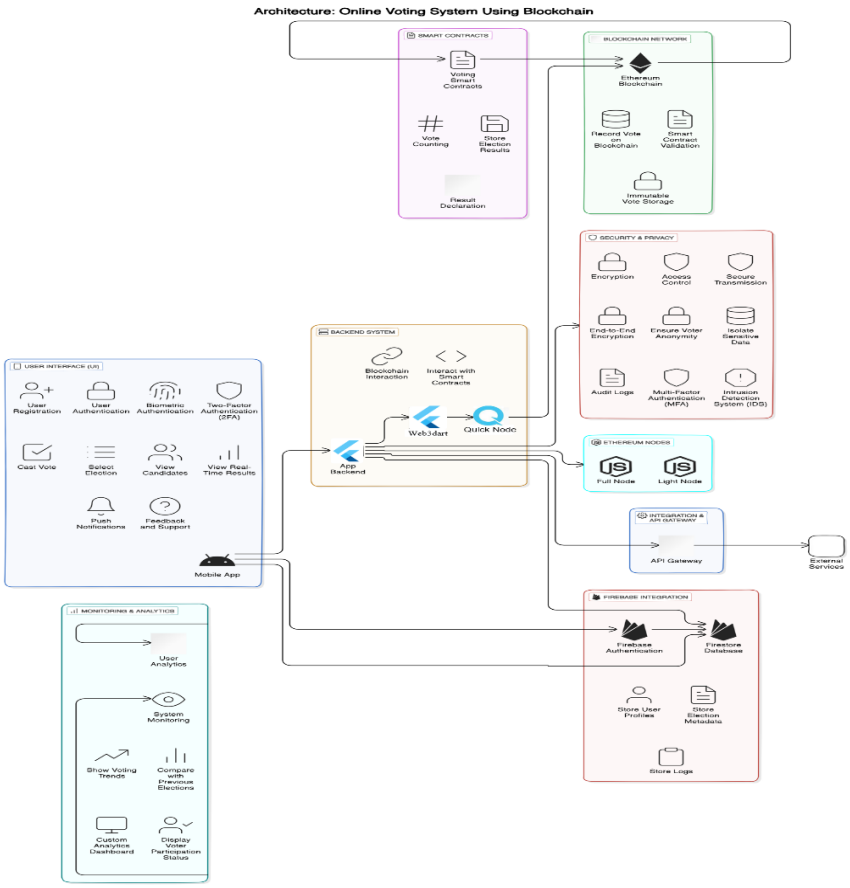

Figure 2: System Architecture

Overall Data Flow:

A user initiates an action (e.g., casting a vote) through the Flutter app. The application logic validates the request and ensures eligibility. The backend (via Firebase and Web3dart.dart) submits the vote to the smart contract on Ethereum Sepolia. The vote is recorded on-chain, while off-chain metadata is concurrently updated in Firebase. Real-time results are displayed in the app, and administrators manage concurrent elections as needed.

Summary of the Proposed System:

By segregating essential vote-recording functions on-chain from ancillary operations handled off-chain, VoteChain achieves:

- **Immutability and Trust:** Permanent, tamper-proof vote recording on the blockchain.
- **High Throughput:** Reduced network congestion and latency via off-chain processing.
- **User-Centric Experience:** A seamless mobile interface with secure MFA and real-time updates.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

- **Dynamic Election Management:** Efficient administration of multiple elections with minimal on-chain load.
- **Enhanced Security:** Robust cryptographic measures and strict access controls to protect sensitive data.

B. Requirements Analysis

VoteChain's design is driven by a comprehensive analysis of both functional and non-functional requirements to address modern electoral challenges.

Functional Requirements

- **Voter Registration & Authentication:** Users register using verifiable credentials and receive unique IDs. MFA (e.g., OTPs, biometrics) reinforces security before voting.
- **Voting Process:** Voters cast ballots for various election types (e.g., Gram Panchayat, Lok Sabha, Vidhan Sabha). Smart contracts ensure eligibility, prevent duplicate voting, and enforce constituency boundaries.
- **Real-Time Results & Transparent Voting:** Votes are tallied on-chain in real time while off-chain systems (e.g., Firebase) capture supplementary metadata for dynamic analytics and graphical visualization.
- **Administrative Control & Dynamic Election Management:** Administrators can create, schedule, and manage multiple elections concurrently. Off-chain candidate and party registrations reduce blockchain load while enabling real-time data modifications.
- **Edge Case Handling & Audit Trails:** The system prevents duplicate voting, restricts voting to designated constituencies, and maintains secure audit logs.

Non-Functional Requirements

- **Performance & Scalability:** The hybrid architecture supports high transaction volumes with minimal latency and is designed to scale for millions of users.
- **Security & Data Integrity:** End-to-end encryption, MFA, blockchain immutability, and regular security audits ensure robust protection against unauthorized access.
- **Usability & Accessibility:** A responsive and intuitive mobile interface accommodates users of varying technical backgrounds through clear visual hierarchies and easy navigation.
- **Cost Efficiency:** Limiting on-chain operations to critical functions minimizes gas fees and overall operational costs.
- **Compliance & Privacy:** The design adheres to data privacy regulations and electoral laws, maintaining secure logs and robust, role-based access controls.
- **Responsiveness:** Sub-second response times provide a smooth and engaging user experience.

C. Technology Selection

The selection of technologies for VoteChain is based on the need for a secure, scalable, and cost-effective electoral system:

- **Blockchain Layer:** Ethereum (Sepolia Testnet) provides robust smart contract capabilities, a well-established network, and integration with QuickNode for efficient connectivity. Solidity employed to develop secure smart contracts for vote recording and tallying.
- **Frontend Development:** Flutter offers a cross-platform framework for building a high-performance, visually engaging mobile application with intuitive UI and smooth animations.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

- **Backend & Database:** Firebase manages voter profiles, election metadata, and audit logs off-chain with real-time data synchronization and scalable storage. QuickNode ensures fast, reliable communication between the mobile app and the Ethereum network for processing vote transactions.
- **Middleware & Integration:** Web3dart.dart serve as the integration layer between the Flutter application and Ethereum, handling API requests, transaction processing, and communication with off-chain databases.
- **Security Enhancements:** Multi-Factor Authentication, Cryptographic Key Management, and End-to-End Encryption integrated across all layers to safeguard user data and ensure the integrity of voting records.

Rationale:
The chosen technologies ensure high performance and scalability while maintaining robust security and cost-effectiveness. Flutter guarantees a consistent user experience; Firebase efficiently handles off-chain data; Ethereum (via QuickNode) provides secure and immutable vote recording; and Web3dart.dart enable seamless integration between all components.

IV. IMPLEMENTATION

VoteChain is a hybrid cross-platform voting application that uses blockchain exclusively for immutable vote recording, while off-chain systems manage supporting functions. The following stepwise implementation outlines key decisions, system flows, and interactions, as illustrated by the accompanying diagrams.

A. Frontend Development

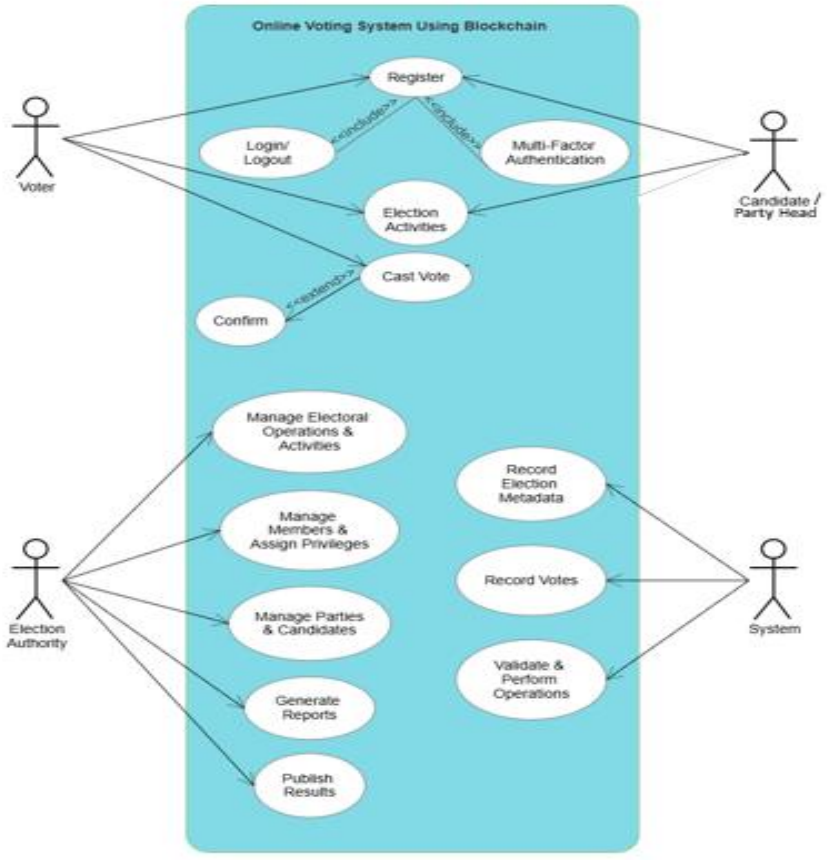

Figure 1: Use Case Diagram

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

- **Framework & UI Design:** Developed using Android-Flutter to deliver a modern, responsive, and intuitive mobile interface. The design includes distinct screens for:
  - **User Registration & Authentication:** Secured via multifactor authentication.
  - **Election Dashboard:** Displays multiple election levels (local, state, national) and includes dedicated views for Party Heads, Candidates, Voters and Election Authorities.
  - **Voting Interface:** Enables users to view candidates, cast votes, and receive real-time feedback.
  - **Result Visualization:** Offers both tabular and graphical representations of election outcomes.
- **User Interaction Flow:** The Use Case Diagram (see Fig. 1) outlines interactions for all key roles—voter, candidate, Party Head, and Admin/Election Authorities—detailing actions such as registration, vote casting, party / candidate application management, and result viewing.

B. Backend and Middleware Integration

- **Middleware Role:** Serves as the secure intermediary between the frontend, blockchain network, and off-chain data store. It validates user actions, ensuring only authenticated and authorized transactions are processed.

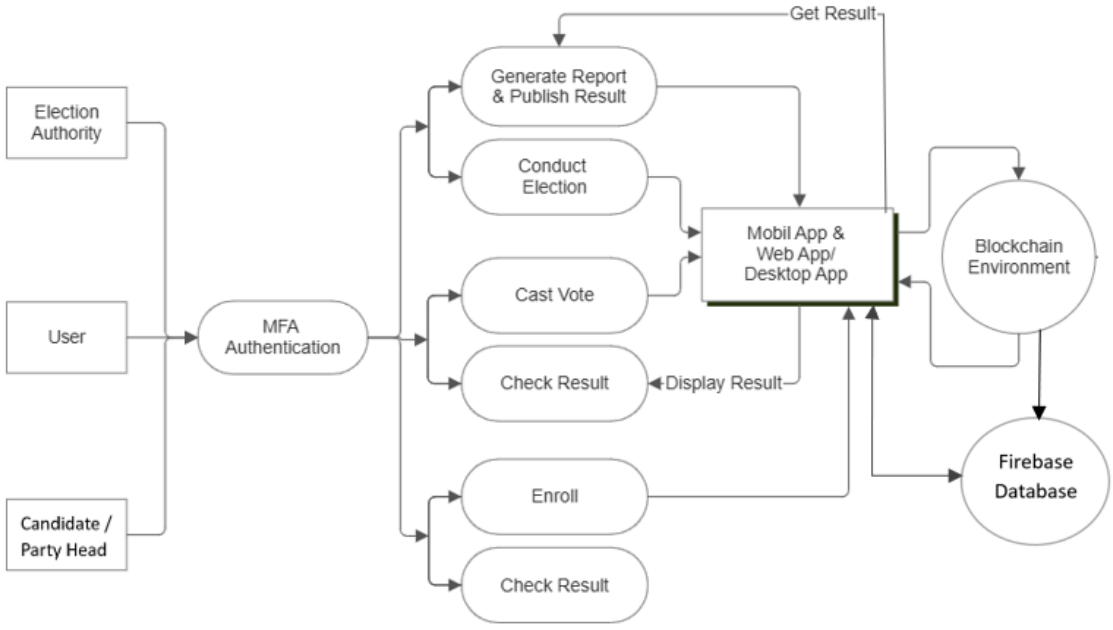

Figure 2: Data Flow Diagram Level 1

- **Data Exchange and APIs:** Provides secure endpoints for synchronizing data and logging transactions. The Data Flow Diagram (DFD Level 1) (see Fig. 2) illustrates how user inputs are processed and routed to the blockchain for vote recording and to the off-chain system for managing metadata.

C. Blockchain Integration

- **Smart Contract Deployment:** A Solidity-based smart contract is deployed on the Ethereum Sepolia testnet via QuickNode. This contract is solely responsible for recording votes and tallying results, thereby reducing gas fees and ensuring transparency.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

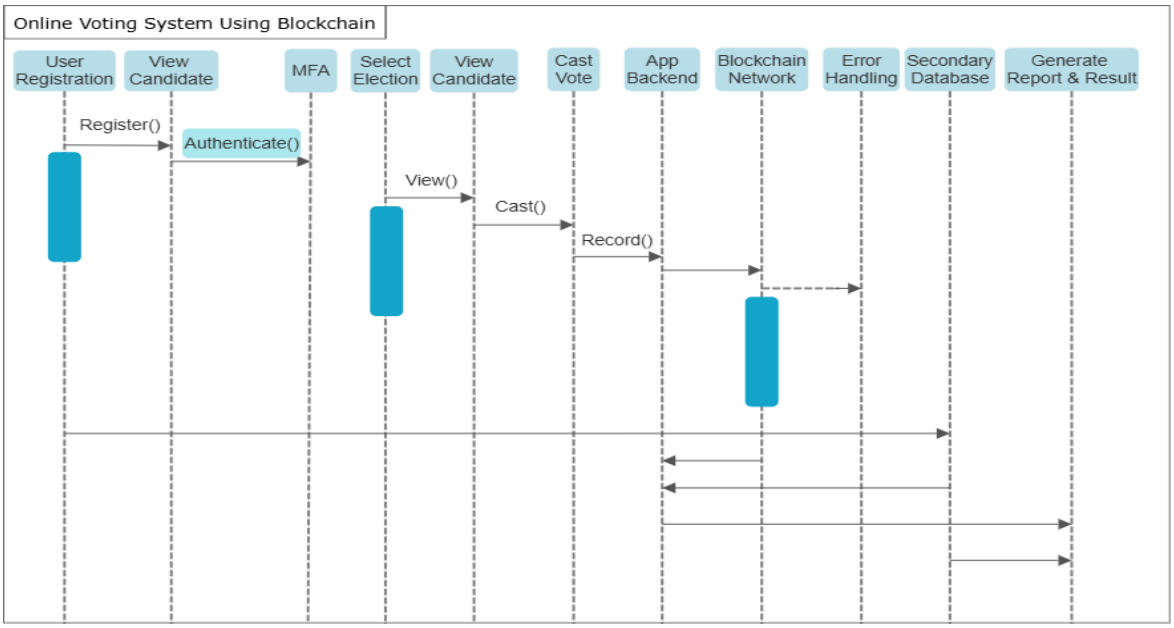

Figure 3: Sequence Diagram (For Citizen - Voting)

- **Interaction with the Application:** The mobile app interacts with the contract using a blockchain library (e.g., web3dart.dart) to execute functions such as casting votes and retrieving vote counts. The Sequence Diagram (see Fig. 3) details the flow between the app, middleware, and smart contract, including confirmation messages sent back to users.

D. Off-Chain Data Management

- **Data Handling Strategy:** All non-critical data—including user profiles, election configurations, party / candidate applications, and detailed logs—is managed off-chain. This approach minimizes blockchain load and ensures high performance during large-scale elections.
- **Security and Scalability:** Robust access controls and encryption safeguard sensitive information, supporting simultaneous elections and real-time updates without exposing internal data structures.

E. Testing and Deployment

- **Testing Protocols:**
  - **Unit and Integration Testing:** Individual modules (UI, middleware, blockchain interface) are rigorously tested, along with end-to-end simulations of the complete voting process.
  - **Security Audits:** Regular audits enforce anti-double-voting measures and check vulnerabilities in the smart contract and backend APIs.
- **Deployment Strategy:** A CI/CD pipeline automates testing and deployment on scalable cloud infrastructure, ensuring high availability. Continuous monitoring and logging enable proactive performance management.

By following this stepwise plan, VoteChain achieves secure, transparent, and cost-effective online voting while ensuring a seamless user experience for Voters, Candidates, Party Heads, and Admin/Election Authorities. The supporting diagrams (Fig. 1, Fig. 2, and Fig. 3) visually clarify the system's data flows and interactions, further reinforcing the robustness of the implementation strategy.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

V. RESULTS AND DISCUSSION

VoteChain's implementation validates that a hybrid blockchain–Firebase architecture can deliver secure, transparent, and cost-efficient online voting. The system—developed using an Android-Flutter mobile application—integrates a Solidity smart contract on the Ethereum Sepolia testnet (accessed via QuickNode) exclusively for immutable vote recording. By offloading user authentication, election metadata, and auxiliary functions to Firebase (Secondary Database), the design reduces on-chain transactions and gas fees by an estimated 40–60%. Furthermore, this approach can reduce overall election costs by 70–80%, saving considerable time and resources that governments can redirect to other critical initiatives, while supporting the scalability required for large-scale elections.

The application's user interface enhances the voting experience by employing multifactor authentication and intuitive navigation across distinct modules. Voters access a secure login, view election details and candidate information on a citizen dashboard, and cast votes on a dedicated voting screen that enforces constituency-specific validations and prevents double voting. Specialized dashboards enable election administrators, party heads, and candidates to manage elections, monitor application statuses, and analyze real-time results through both list and graphical formats. Integrated screenshots of key screens (Fig. 1, Fig. 2, Fig. 3, Fig. 4, Fig. 5, Fig. 6, and Fig. 7) illustrate the system's operational transparency and seamless flow.

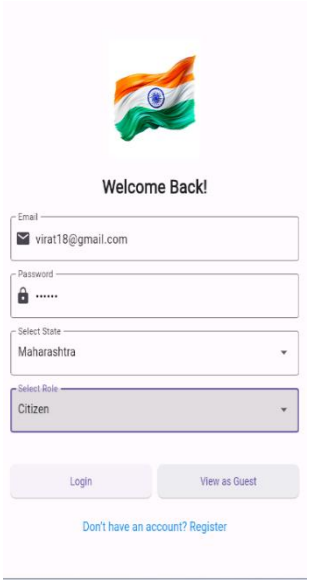

Figure 1:
Login Screen

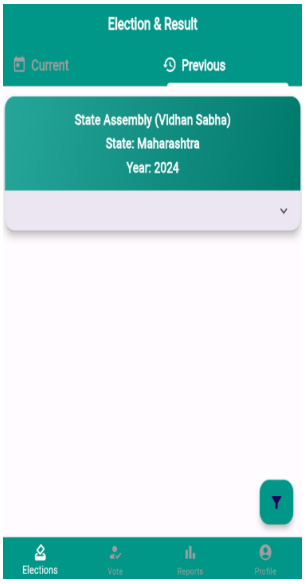

Figure 2
Citizen Dashboard

Figure 3:
Voting Screen

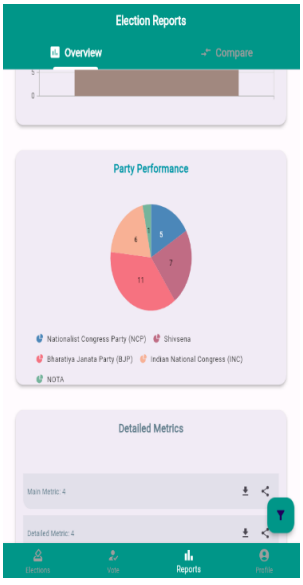

Figure 4:
Reports Screen

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:07/Issue:03/March-2025 Impact Factor- 8.187 www.irjmets.com

Figure 5
Admin Dashboard

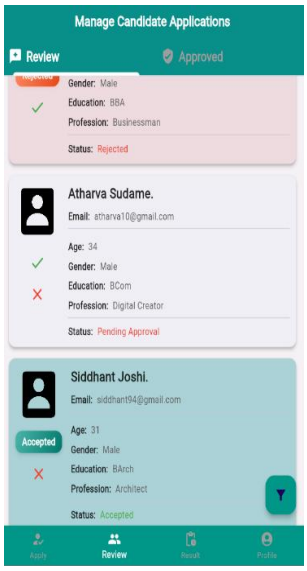

Figure 6:
Party Head Dashboard

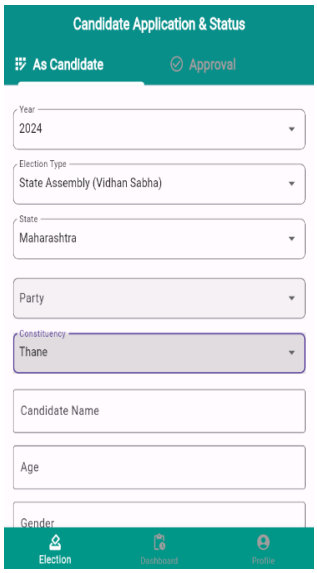

Figure 7:
Citizen Dashboard

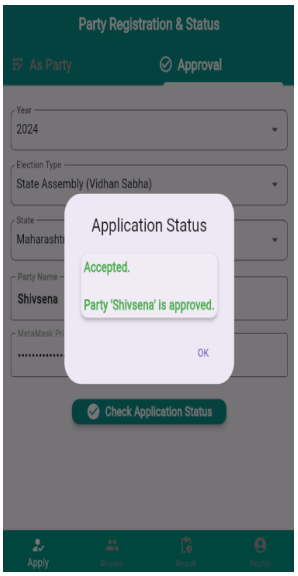

Figure 8:
Party-Application-Status Screen

From a backend perspective, the dual-layer approach proves effective: blockchain records provide immutability and verifiability of votes, while Firebase's hierarchical data structure—organized by state, election year, and election name—facilitates complex queries and real-time synchronization. This separation enhances system performance under high user loads and supports various election types (e.g., local, state, national) with dynamic candidate-party relationships. In addition, robust security measures, including role-based access control and multifactor authentication, further safeguard the voting process against manipulation. The system's modularity also allows for future enhancements, such as advanced consensus algorithms and machine-learning-based anomaly detection.

VI. CONCLUSION

Vote Chain presents a novel, hybrid approach to modernizing electoral systems by confining blockchain use solely to the immutable recording of votes while managing ancillary functions off-chain via Firebase. This focused application of blockchain minimizes operational overhead and transaction costs, ensuring both high throughput and transparency even in densely populated electoral environments.

Key security features, such as multifactor authentication and role-based access control, safeguard against unauthorized access and double voting. The Firebase-backed data structure supports dynamic election management and real-time result visualization across local, state, and national elections. Although the current implementation effectively addresses many challenges of digital voting, further optimization of smart contract execution and enhanced privacy measures remain promising avenues for future research. Empirical validation through pilot studies and iterative user testing, coupled with the establishment of standardized evaluation frameworks and regulatory guidelines, will be essential for broader adoption.

In summary, Vote Chain lays a robust foundation for the next generation of digital democracy by addressing critical issues in electoral integrity, cost efficiency, and scalability. Continued interdisciplinary collaboration and targeted research will be imperative to transform this promising model into a globally applicable solution for secure, transparent, and accessible elections.

REFERENCES

[1] Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerjee, Madhuri Chavan, "Blockchain Enabled Online-Voting System", ITM Web of Conferences, 32, 03018, 2020.

[2] Wenbin Zhang, Sheng Huang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra, "A Privacy-Preserving Voting Protocol on Blockchain", Journal of Information Security, 9(1), 54-67, 2018.

[3] Stephan Neumann, Oksana Kulyk, Melanie Volkamer, "A Usable Android Application Implementing Distributed Cryptography for Election Authorities", Journal of Cryptography, 7(2), 120-130, 2014.

[4] Jae-Geun Song, Sung-Jun Moon, Ju-Wook Jang, "A Scalable Implementation of Anonymous Voting over Ethereum Blockchain", IEEE Access, 9, 37930-37942, 2021.

[5] Yulia Bardinova, Konstantin Zhidanov, Sergey Bezzateev, Mikhail Komarov, Aleksandr Ometov, "Measurements of Mobile Blockchain Execution Impact on Smartphone Battery", Journal of Mobile Computing, 8(1), 58-67, 2019.

[6] David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb, "Decentralized Voting Platform Based on Ethereum Blockchain", International Conference on Decentralized Applications and Infrastructures (DAPPS), 65-70, 2020.

[7] D. Dwijesh Kumar, D. V. Chandini, Dinesh Reddy, "Secure Electronic Voting System using Blockchain Technology", Proceedings of the 2020 Blockchain Conference, 112-119, 2020.

[8] Saad Moin Khan, Aansa Arshad, Gazala Mushtaq, Aqeel Khalique, Tarek Husein, "Implementation of Decentralized Blockchain E voting", International Journal Applications, 182(20), 1-5, 2018.

[9] G. Kalaiyarasi, T. Narmadha, K. Balaji, V. Naveen, "E-Voting System in Smart Phone Using Mobile Application", International Journal of Advanced Research in Computer Science, 11(4), 41 48, 2020.

[10] Hussam Saeed Musa, Moez Krichen, Adem Alpaslan Altun, Meryem Ammi, "Survey on Blockchain-Based Data Storage Security for Android Mobile Applications", Journal of Blockchain Research, 5(3), 102-110, 2019.