IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁒ Peer-reviewed & Refereed journal ⁒ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412148

E-VOTING SYSTEM USING BLOCKCHAIN

Ananya Y.A.[1], Dr. Madhu H.K.[2]

Department of MCA, BIT, Bangalore, India[1]

Professor and Head, Department of MCA, BIT, Bangalore, India[2]

Abstract: The credibility of democratic systems relies heavily on the integrity and transparency of electoral processes. Traditional voting mechanisms, including paper ballots and electronic voting machines, suffer from several drawbacks such as centralized control, susceptibility to manipulation, lack of transparency, and delayed result declaration. To address these limitations, this paper proposes a Blockchain-Based E-Voting System that leverages decentralized ledger technology to ensure secure, transparent, and tamper-proof elections. The system utilizes Ethereum-compatible blockchain networks and smart contracts written in Solidity to automate vote validation, storage, and counting. A modern frontend built using React, TypeScript, and Vite provides an intuitive voting interface, while Supabase serves as a cloud backend for authentication, election metadata, and audit logging. Wallet-based voter authentication using MetaMask ensures secure participation and prevents duplicate voting. Experimental evaluation demonstrates that the proposed system significantly improves trust, efficiency, and transparency while reducing operational overhead. The results validate blockchain as a viable solution for secure digital voting systems.

Keywords: Blockchain, E-Voting, Smart Contracts, Ethereum, Solidity, Supabase

I. INTRODUCTION

The electoral voting process is one of the most critical pillars of democratic governance. Despite advancements in digital technologies across various sectors, voting systems continue to rely heavily on centralized and semi-digital approaches. These traditional systems are vulnerable to manipulation, lack verifiability, and often generate public distrust.

Blockchain technology introduces decentralization, immutability, and cryptographic security, making it a suitable foundation for modern voting systems. By recording votes as irreversible transactions on a distributed ledger, blockchain eliminates single points of failure and enhances public confidence in election outcomes.

1.1 Project Description

The proposed Blockchain-Based E-Voting System is a decentralized web-based application that enables secure online voting using blockchain technology. Votes are cast through smart contracts deployed on Ethereum-compatible networks, ensuring that each vote is immutable and verifiable. Supabase manages election-related metadata and audit logs, while MetaMask enables wallet-based voter authentication.

1.2 Motivation

Growing concerns about election fraud, delayed results, and lack of transparency motivate the development of a decentralized voting system. Blockchain removes reliance on central authorities and ensures public verifiability without compromising voter privacy.

II. LITERATURE SURVEY

Electronic voting systems have been extensively researched to overcome the drawbacks of traditional paper-based elections and centralized electronic voting machines. Although electronic systems improve efficiency, they often suffer from issues such as lack of transparency, centralized control, security vulnerabilities, and reduced public trust. To address these challenges, researchers have explored blockchain technology as a foundation for secure and transparent voting systems.

Patidar and Jain (2019) proposed a decentralized e-voting system using Ethereum blockchain and smart contracts. Their approach eliminates central authority and ensures vote immutability using MetaMask-based authentication. While the system improves transparency and security, it lacks scalability and real-time result visualization.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁘ Peer-reviewed & Refereed journal ⁘ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412148

Adiputra et al. (2018) introduced a blockchain-based voting system combined with cryptographic techniques to ensure vote confidentiality. The system improves data integrity and privacy but relies on centralized election authorities, which limits complete decentralization.

Bulut et al. (2019) presented a layered blockchain voting architecture designed to improve scalability and performance in large elections. Although the approach enhances system reliability, it requires complex identity management mechanisms and significant infrastructure support.

2.1 Existing System vs Proposed System

Existing Voting System

Traditional voting systems primarily rely on paper ballots or Electronic Voting Machines (EVMs) managed by centralized authorities. Although these systems are widely used, they suffer from several limitations. Votes are stored in centralized databases, making them vulnerable to tampering, insider threats, and cyberattacks. The counting process is often slow and requires significant manpower and logistics. Additionally, voters have no direct way to verify whether their vote was recorded or counted correctly, which leads to trust issues and lack of transparency.

Proposed Blockchain-Based E-Voting System

The proposed system replaces centralized vote storage with a decentralized blockchain network. Each vote is recorded as a cryptographically signed transaction on the blockchain through Solidity smart contracts, ensuring immutability and transparency. Wallet-based authentication using MetaMask guarantees voter identity without exposing personal information. A cloud backend (Supabase) manages election metadata, authentication, and audit logs, while vote casting and counting are fully automated on-chain. This approach eliminates manual intervention, reduces cost, prevents fraud, and builds public trust.

SYSTEM ARCHITECTURE DIAGRAM

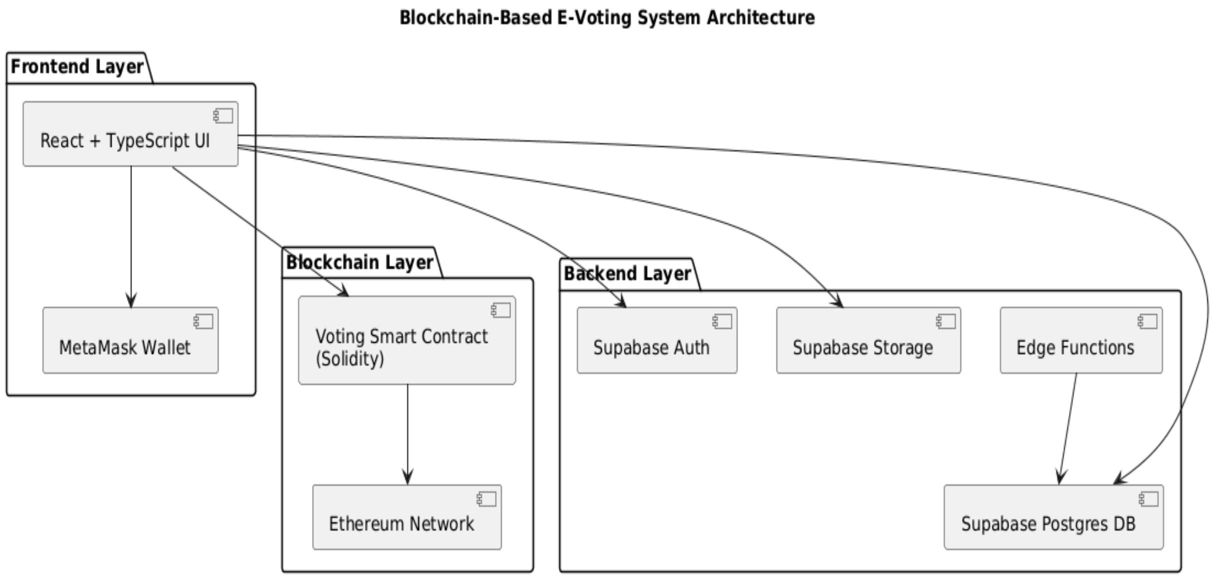

Fig.3.1 System Architecture Diagram

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.1412148

III. SYSTEM DESIGN

3.1 Data flow diagram

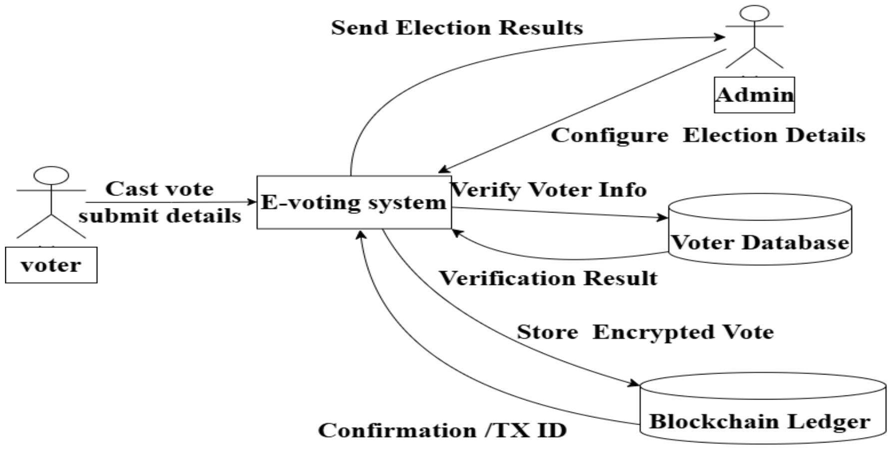

Fig. 3.1.1 Level 0 Data Flow Diagram

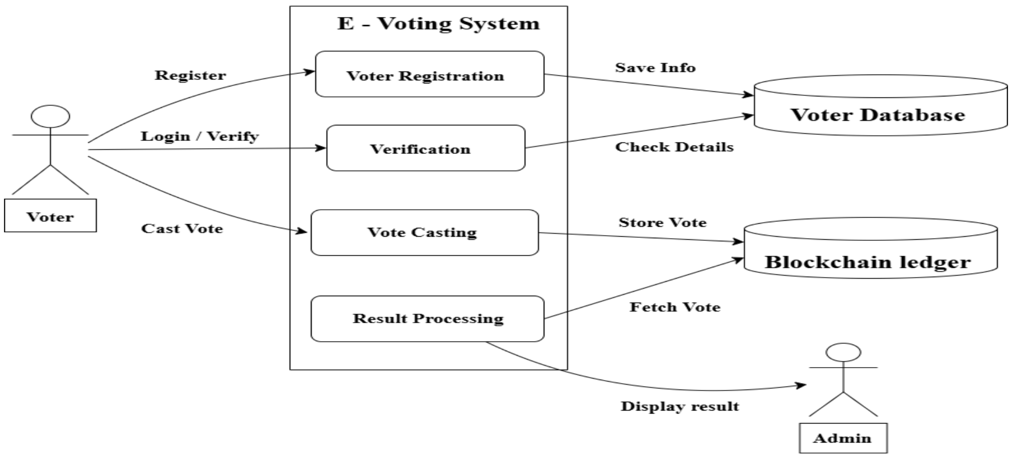

Fig. 3.1.2 Level 1 Data Flow Diagram

3.2 Use Case diagram

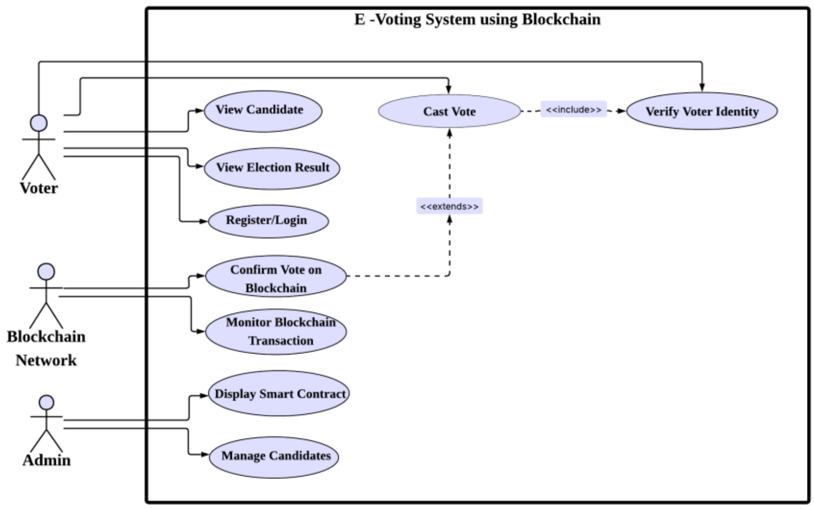

Fig 3.2.1 use case diagram foe e -voting system

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⵗ Peer-reviewed & Refereed journal ⵗ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412148

IV. IMPLEMENTATION DETAILS

The system is implemented using a three-layer architecture:
Frontend Layer

- Developed using React + TypeScript + Vite
- Styled with Tailwind CSS and Radix UI
- Wallet integration handled using ethers.js v6
- Enables users to connect wallets, view elections, cast votes, and see real-time results

Blockchain Layer

- Smart contracts written in Solidity (Voting.sol)
- Compiled, tested, and deployed using Hardhat
- Supports networks such as Hardhat Local, Sepolia, and Polygon Amoy
- Manages candidate registration, vote casting, and vote counting

Backend Layer

- Built using Supabase
- Uses PostgreSQL for election and candidate data
- Supabase Auth for admin authentication
- Edge Functions for secure backend operations
- Stores audit logs and transaction references

4.1 System Modules and Workflow

System Modules

User (Voter) Module

- Wallet connection via MetaMask
- Election viewing
- Candidate selection
- Vote casting

Admin Module

- Admin authentication
- Election creation and scheduling
- Candidate management
- Vote monitoring and analytics

Smart Contract Module

- Candidate registration
- Vote validation
- Prevention of double voting
- Event emission for real-time updates

Database and Audit Module

- Stores election metadata
- Maintains vote logs and transaction hashes
- Enables audit and verification

Workflow

- Admin creates an election and adds candidates
- Voter connects MetaMask wallet
- Voter selects election and candidate
- Vote is signed and sent as a blockchain transaction
- Smart contract validates and records vote
- Blockchain event triggers UI update
- Supabase logs vote metadata
- Results update in real time

4.2 Testing Overview

Unit Testing

- Frontend components tested using Vitest
- Smart contract functions tested using Hardhat + Mocha + Chai

Integration Testing

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⩰ Peer-reviewed & Refereed journal ⩰ Vol. 14, Issue 12, December 2025

DOI: 10.17148/IJARCCE.2025.1412148

- Wallet–Blockchain interaction verified
- Frontend–Backend data flow tested

System Testing

- Complete voting workflow tested end-to-end

Security Testing

- Double voting prevention
- Unauthorized access checks
- Smart contract validation

Performance Testing

- Transaction confirmation time analysis
- UI response under multiple users

User Acceptance Testing (UAT)

- Validates usability and user experience

V. RESULTS AND DISCUSSION

The proposed blockchain-based e-voting system was successfully implemented and evaluated using Ethereum-compatible blockchain networks. The system enabled secure wallet-based voter authentication, accurate vote casting, immutable storage of votes on the blockchain, and real-time result visualization. Smart contracts strictly enforced voting rules such as allowing only one vote per wallet and validating candidate selections. Any attempt at duplicate voting was automatically rejected, demonstrating the effectiveness of the system in preventing common electoral frauds.

Supabase was used as a backend service to manage election metadata, candidate information, and audit logs. While vote data was securely stored on-chain, off-chain logs improved accountability by recording transaction details such as timestamps and transaction hashes. The hybrid architecture balanced decentralization with efficient system management. Performance testing showed that vote confirmation times varied depending on the blockchain network, with local Hardhat providing instant results and public test networks showing acceptable latency for small to medium-scale elections. Compared to traditional voting systems, the proposed solution reduced administrative effort, improved transparency, and increased voter trust through public verifiability of results.

VI. CONCLUSION

This paper presented a secure, transparent, and decentralized blockchain-based e-voting system designed to overcome the limitations of traditional voting mechanisms. By integrating Solidity smart contracts, wallet-based authentication, and a modern web interface, the system eliminated centralized vulnerabilities and ensured election integrity. Automated vote validation and counting reduced human intervention and operational overhead. The successful implementation and evaluation confirm that blockchain technology is a promising solution for building trustworthy and efficient digital voting platforms

VII. FUTURE WORK

Future enhancements can further strengthen the system's capabilities. The integration of zero-knowledge proof techniques can provide stronger voter anonymity while maintaining verifiability. Biometric or government-issued digital identity authentication can enhance voter validation and prevent wallet misuse. Mobile application development and the adoption of Layer-2 blockchain solutions can improve accessibility, scalability, and cost efficiency. Additional improvements such as advanced analytics, multi-language support, and DAO-based election governance can make the system suitable for large-scale real-world elections.

REFERENCES

[1]. K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," Proc. 10th Int. Conf. Computing Communication and Networking Technologies (ICCCNT), 2019.

[2]. C. K. Adiputra, R. Hjort, and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," World Conf. Smart Trends in Systems, Security and Sustainability, 2018.

[3]. R. Bulut, A. Kantarci, S. Keskin, and S. Bahtiyar, "Blockchain-Based Electronic Voting System for Elections," Int. Conf. Computer Science and Engineering, 2019.

[4]. G. Dagher, P. Babu, M. Milojkovic, and J. Mohler, "BroncoVote: Secure Voting System Using Ethereum's Blockchain," Int. Conf. Information Systems Security and Privacy, pp. 96–107, 2018.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 14, Issue 12, December 2025
DOI: 10.17148/IJARCCE.2025.1412148

[5]. A. Singh and K. Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology," Int. Conf. Computing, Power and Communication Technologies, 2019.
[6]. L. A. Ajao et al., "Blockchain Integration with Multimodal Biometric Authentication for Secure E-Voting," IEEE Access, vol. 13, 2025.
[7]. E. Tyagi et al., "Next-Generation E-Voting Security using Blockchain Technology," Int. Conf. Intelligent and Secure Engineering Solutions, 2025.
[8]. R. Barelli, M. D'Onghia, and S. Longari, "Toward Secure Electronic Voting: A Survey on E-Voting Systems and Attacks," IEEE Access, vol. 13, 2025.