ijamrsd.com
JAMRSD
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal | Bi-monthly | Open Access

BLOCKCHAIN FOR BHARAT: SECURE & IMMUTABLE NRI VOTING SYSTEM

Disha Pardeshi[1], Sujata Sathe[2], Viha Bakshi[3], Ananya Mary Sebastian[4]
[1,3,4] *Student of Computer Science Department, Fergusson College (Autonomous), Pune, India.*
Email: pardeshidisha2505@gmail.com[1], bakshiviha2615@gmail.com[3], ananyamarysebastian05@gmail.com[4]
[2] *Faculty of Computer Science Department, Fergusson College (Autonomous), Pune, India.*
Email: sujata.sathe@fergusson.edu

Abstract
The growing need for secure and transparent electoral systems highlights the challenges faced by Non-Resident Indian (NRI) voters. Current rules requiring physical presence at polling stations limit participation, despite rising registrations. In our proposed blockchain-based voting framework, votes are transmitted through a secure virtual private network (VPN) and authenticated at the Election Commission of India (ECI) gateway node. After authentication, the votes are verified across multiple blockchain nodes using a consensus mechanism. Once validation is completed, the votes are permanently recorded in the distributed ledger, ensuring that they cannot be altered or removed. Smart contracts are employed to automate the vote-counting process, reducing manual intervention and minimizing the possibility of human error. The final election results are then made available through the ECI dashboard, enabling transparency and easy verification by authorized stakeholders.The proposed framework aims to improve accessibility for Non-Resident Indian (NRI) voters by enabling secure remote participation while preserving voter anonymity. By strengthening trust in the electoral system and encouraging wider participation, the solution supports improved electoral integrity. Overall, the integration of blockchain technology into the voting process contributes toward building a more transparent, secure, and inclusive democratic system in India.
Keywords: Blockchain, NRI Voting, Distributed Ledger, Electoral Integrity, Consensus Mechanism, Immutability, Voter Anonymity.

► *Corresponding Author: Disha Pardeshi*

[1] Introduction

Voting is the fundamental element of any democratic system, as it allows citizens to actively participate in governance by electing their representatives. In India, both paper-based and electronic voting mechanisms have been widely used to conduct elections. Despite their widespread adoption, these traditional approaches continue to face several challenges. Issues such as susceptibility to tampering, limited transparency, delays in result declaration, and reliance on centralized control raise concerns about the overall credibility of the electoral process.

These challenges are more pronounced for Non-Resident Indians (NRIs). Although a significant number of NRIs are registered as voters, their actual participation in elections remains relatively low. This can be attributed to the requirement of physical presence in India or dependence on postal voting systems, which are often time-consuming and unreliable. Additionally, long-distance travel, geographical dispersion, and unforeseen situations such as global health emergencies further restrict the ability of NRIs to participate effectively in elections.

In this context, blockchain technology offers a potential alternative for addressing the limitations of conventional voting systems. Blockchain is a decentralized and distributed ledger technology in which data is stored across multiple interconnected nodes rather than a single authority. Its core features include decentralization, immutability, cryptographic security, and consensus-based verification. These characteristics make blockchain suitable for applications that require high levels of transparency, trust, and security.

When applied to an electronic voting system, blockchain enables votes to be securely recorded and timestamped in a tamper-resistant ledger. Each vote can be independently verified without revealing voter identity, thereby maintaining anonymity while ensuring data integrity. This approach reduces the risk of manipulation and enhances confidence in the electoral process for both voters and election authorities.

While several studies have proposed blockchain-based voting solutions, many of these models remain conceptual or fail to address practical concerns such as scalability, usability, and deployment in real-world election scenarios. As a result, there is a need for implementable frameworks that demonstrate secure and transparent voting beyond experimental settings.

To address this requirement, this paper presents a blockchain-based voting system tailored for NRI voters. The proposed framework incorporates secure voter authentication, transparent vote recording, and verifiable vote tallying through a distributed blockchain network. The objective of this study is to demonstrate how blockchain technology can support a reliable, transparent, and inclusive electoral process, thereby strengthening democratic participation and electoral integrity in India.

[2] Literature Review

Evolution of Voting Technologies

[1],[2] The transition from traditional paper-based voting to electronic voting systems was primarily driven by the need to improve efficiency, reduce manual errors, and accelerate result processing. However, several studies indicate that conventional electronic voting systems are limited by centralized control, lack of transparency, restricted auditability, and vulnerability to manipulation. As a result, voter trust is weakened, and doubts are often raised about the credibility of election results.

[5] Further research highlights that such limitations become more critical during exceptional situations such as pandemics, as well as for elderly voters with mobility challenges and citizens residing in remote or overseas locations. These observations have encouraged the exploration of decentralized and remote-access voting solutions.

Blockchain-Based Voting Approaches

[3] Blockchain technology has been widely studied as a potential foundation for secure electronic voting due to its decentralized architecture, immutability, and cryptographic security mechanisms. Nandimath and Mandape propose a blockchain-based e-voting system integrated with Aadhaar authentication to ensure secure voter registration and tamper-resistant vote storage.

[4] Similarly, Reddy et al. introduce a blockchain-enabled voting framework that leverages Aadhaar credentials to minimize voter impersonation and vote manipulation.

[6] Other studies extend blockchain voting systems by incorporating additional components. Blockchain-powered e-voting systems using biometric authentication and decentralized storage through IPFS have been proposed to enhance privacy and data availability.

[7] Consensus mechanisms such as Practical Byzantine Fault Tolerance (PBFT) have also been explored to improve system reliability and resistance to malicious nodes.

[8] Additionally, smart contracts have been used to automate election processes such as vote casting and tallying, reducing human intervention and operational errors.

Security, Privacy, and Trust Considerations

[1] Security and voter privacy are central concerns across blockchain-based voting research. Existing studies emphasize the use of cryptographic techniques such as hashing, encryption, and digital signatures to protect vote integrity and prevent unauthorized modifications. The immutable nature of blockchain further strengthens trust by ensuring that once votes are recorded, they cannot be altered or deleted.

[1], [6] However, researchers caution that transparency must be carefully balanced with voter anonymity. Several studies recommend separating voter authentication from vote storage to prevent linking voter identities to ballots. Despite these measures, achieving complete privacy while maintaining transparency and verifiability remains a key challenge.

Studies Incorporating Existing Models and Comparative Analysis

[2] Survey and review-based studies play a significant role in evaluating blockchain-based voting systems. Kumar et al. provide a comprehensive survey of existing blockchain-enabled e-voting models, comparing them based on security, transparency, scalability, and consensus mechanisms.

[1] Similarly, a detailed review published in *Symmetry* analyses the feasibility and suitability of blockchain techniques for voting applications, identifying recurring challenges such as scalability constraints and privacy risks.

[6], [8] Several implementation-focused studies explicitly cite and build upon previously proposed models, extending them with biometric authentication, IPFS-based storage, or smart contract automation. These works primarily present incremental improvements rather than entirely new architectures, demonstrating strong reliance on existing models for system design decisions.

Identified Research Gap

[2], [5] Although the literature establishes blockchain as a promising solution for secure and transparent electronic voting, most existing systems remain conceptual or limited to prototype implementations. Critical challenges such as scalability under large voter populations, usability for non-technical users, accessibility for elderly and overseas voters, and real-world deployment constraints are often insufficiently addressed. These limitations highlight the need for a practical, user-friendly, and secure blockchain-based voting system that can be evaluated in realistic scenarios, particularly for remote and NRI voting applications.

[3] Problem Statement

1. **Physical inaccessibility for NRIs-** Many NRIs cannot physically reach polling stations, which excludes a large overseas population from participating in elections.
2. **Very low turnout despite registrations-** Even when NRIs register, actual voting rates are extremely low (examples from recent elections show registrations in thousands but votes cast in very small numbers), indicating that registration alone doesn't solve participation.
3. **Postal / Electronically Transmitted Postal Ballot (ETPB) limitations-** Postal ballots (and proposed ETPB schemes) suffer from delays, delivery vulnerabilities, and administrative complexity that reduce reliability and trust.
4. **Legal and administrative gaps-** Although proposals (e.g., proxy voting, ETPBS) and bills have been discussed, many reforms lapsed or remain pending leaving no robust, approved system for large-scale overseas voting.

5. Security & transparency concerns with remote/online voting- Conventional online or postal methods lack strong end-to-end verifiability and can introduce new attack surfaces; single vulnerabilities in electronic systems can result in large-scale manipulations if not properly designed. Blockchain is proposed as a mitigation, but research stresses caution and careful design.

6. Practical deployment challenges for secure electronic solutions- Real-world issues such as usability for diverse voters, scalability, costs (e.g., gas fees on public chains), and integration with secure authentication remain unresolved, so many blockchain/e-voting proposals are still prototypes rather than production systems.

[4] Objectives

1. To enable secure remote voting for NRI citizens worldwide

Provide a digital platform that allows eligible Indian citizens living abroad to cast votes without needing to travel physically or rely on postal ballots.

2. To ensure voter anonymity while maintaining vote verifiability

Use cryptographic techniques and blockchain features so that votes cannot be linked to voter identities, but each vote can still be publicly verified.

3. To create a tamper-proof and immutable voting ledger

Record every vote on a decentralized blockchain network to eliminate risks of manipulation, deletion, or alteration.

4. To automate and simplify the vote-counting process

Utilize smart contracts to automatically tally votes, reducing human error and enabling transparent, real-time auditability.

5. To develop a voting system that users can trust and that allows transparent verification

Ensure that all stakeholders including voters and authorities can verify the integrity of the election process at every stage.

6. To design a prototype that demonstrates the feasibility of blockchain in large-scale Indian elections

Show how the model developed for NRIs can later be expanded for domestic use, including elderly voters, people with disabilities, or citizens residing in remote areas.

[5] Proposed System

This section describes the prototype implementation of a blockchain-based NRI (Non-Resident Indian) voting system which we build as a part of our project. We built an easy prototype which demonstrates how a combination of Ethereum smart contracts, a local development blockchain (Ganache), a browser wallet (MetaMask), and a lightweight frontend can enable secure, transparent remote voting for NRIs.

5.1 Explanation of the modules

1. Frontend (Presentation Layer)

- Technology: HTML, CSS, JavaScript (Web3.js).
- Responsibilities: Present the voting UI (candidate dropdown, connect wallet button, vote button, live vote counts), request wallet access, format user inputs, call smart contract methods, and read contract state to display results.

2. Wallet (MetaMask)

- Technology: MetaMask browser extension.

- Responsibilities: Manage private keys on the client, present transaction signing dialogs to the voter, and inject window.ethereum provider so the frontend can request accounts and send signed transactions.

3. Smart Contract Layer (Voting.sol)

- Technology: Solidity.
- Responsibilities: Core on-chain logic to store candidate list, accept valid votes, prevent double-voting (mapping hasVoted), and expose read functions (votesReceived, candidatesCount) for transparent tallying.

4. Blockchain Node (Ganache / Ethereum)

- Technology: Ganache (development) or Ethereum node/Infura/Alchemy (production).
- Responsibilities: Host the ledger, accept JSON-RPC calls, mine transactions (instant in Ganache), and persist contract state.

5. Migration & Deployment (Truffle)

- Technology: Truffle Suite.
- Responsibilities: Compile Solidity contracts, run deployment scripts (migrations), and generate ABI & artifact files used by the frontend.

6. Off-chain Registration & Authentication (Optional for prototype)

- Technology: Server (Node.js) + database + identity providers.
- Responsibilities: Register eligible NRI voters (validate identity documents), bind verified identities to blockchain addresses (for production, use secure KYC and audited mapping). In the prototype this is simulated or minimally implemented.

7. Admin / Registrar Interface (Optional for prototype)

- Responsibilities: Manage candidate list, start/stop elections, export logs/audits. In the prototype candidate list is set at deploy time via migration script.

5.2 Working Process (Step-by-Step)

This subsection explains the full lifecycle from voter registration to result display in the prototype and in a productionized design.

->Voter Registration (prototype vs production)

- **Prototype:**
  - Registration is simulated. The developer deploys contract and uses Ganache accounts imported into MetaMask to represent voters.
- **Production:**
  - Voter registers via an official portal. Identity verification (KYC) is performed using government databases (passport, Aadhaar, biometrics). After verification, the system issues a single-use credential or registers a canonical address for the voter (e.g., through a signed certificate). This off-chain binding maps the verified identity to a blockchain address that will be permitted to vote.

-> Authentication

- **Client authentication:** Voter authenticates locally with MetaMask (unlocking the wallet).
- **System authentication:** Before voting, the portal verifies that the MetaMask address is enrolled and authorized. In production, this would be a server check ensuring only enrolled addresses vote.

->Smart Contract for Vote Storage

The core logic of the voting system is implemented using a Solidity smart contract. The contract ensures that:

- Each Ethereum address can vote only once
- Votes are stored immutably on the blockchain
- Only valid candidates can receive votes
- The smart contract (deployed during migration) holds:
  - *bytes32[] candidates* — list of candidates.
  - *mapping(bytes32 => uint) votesReceived* — vote counts per candidate.
  - *mapping(address => bool) hasVoted* — prevents double voting.
  - *candidatesCount* for quick iteration when reading results.
- Contract functions:
  - *voteForCandidate(bytes32 candidate)* — checks *!hasVoted[msg.sender]* and *validCandidate(candidate)*, then increments *votesReceived* and marks voter.
  - *validCandidate(bytes32)* and getters *for votesReceived*.

->Vote Casting (frontend → MetaMask → blockchain)

1. Voter opens the frontend and clicks **Connect Wallet** (MetaMask prompts to approve account access).
2. Frontend loads candidate list from contract (*via candidatesCount() and candidates(i)*).
3. Voter selects a candidate (UI dropdown or button).
4. Frontend *calls votingContract.methods.voteForCandidate(hexCandidate).send({from: account})*.
5. MetaMask shows confirmation dialog; voter approves.
6. The signed transaction is submitted to the blockchain node (Ganache in prototype; a production RPC node or provider in deployment).
7. Node mines the transaction (instant in Ganache). The smart contract executes, updates *votesReceived* and *hasVoted*.

-> Transaction on Blockchain

- Transactions are immutable and logged; each successful vote yields a transaction hash and block receipt. These records are usable for audit and verification.
- For each transaction, the frontend can read the receipt and display status (pending, confirmed).

-> Counting & Result Display

- **On-chain counting:** The smart contract maintains live tallies in *votesReceived*.
- **Frontend display:** The UI *calls votesReceived*(candidate) for each candidate and displays counts. Optionally, a *getAllVotes()* view function returns all candidates and counts in a single call for efficiency.
- **Auditing:** Anyone with the contract address and ABI can query the blockchain to verify results independently.

[6] Advantages of the Proposed System

1. Decentralized Architecture

The proposed voting system is built on a decentralized blockchain network, eliminating the dependence on a single authority. This ensures that no central organization can manipulate, alter, or control the voting process, thereby increasing trust and fairness in elections.

2. Tamper-Proof Data Storage

All votes recorded on the blockchain are immutable, meaning they cannot be edited, deleted, or altered once submitted. This prevents fraudulent activities such as vote manipulation, duplicate voting, or unauthorized access, making the system inherently secure.

3. Enhanced Transparency

Since every transaction (vote) is stored on a public or permissioned ledger, the system ensures complete traceability. Election authorities are able to verify vote counts while voter identities remain protected, maintaining transparency without compromising confidentiality.

4. Remote Accessibility for NRIs

The proposed system enables Non-Resident Indian (NRI) voters to cast their votes remotely from any location across the globe, without the need to visit polling stations or Indian consulates. This feature addresses the practical difficulties faced by NRIs due to geographical distance and travel constraints.

5. Faster Vote Counting and Results

Blockchain technology supports real-time vote recording and automated tallying through smart contracts. This removes the delays associated with physical ballot handling and manual counting processes. Consequently, election results can be generated more quickly while remaining accurate and verifiable.

6. High Security through Cryptography

The proposed voting system employs cryptographic mechanisms such as hashing and digital signatures to authenticate voters and validate voting transactions. These techniques help ensure data integrity and protect the confidentiality of voting information. In addition, blockchain wallets securely manage private keys, allowing only authorized users to cast votes without exposing voter identities. Together, these measures reduce the risk of unauthorized access and enhance the overall security of the voting process.

7. Increased Voter Trust

Transparency, decentralization, and immutability are key characteristics of the blockchain-based voting framework. These features allow voters to verify that their votes have been recorded correctly and cannot be altered.

8. Reduces Human Errors

Automation of critical processes such as vote submission, verification, and counting minimizes the likelihood of errors commonly associated with manual systems. Issues such as miscounted votes, lost ballots, or administrative inconsistencies can be significantly reduced, contributing to a more reliable and efficient election process.

9. Scalable for Future Elections

The system can be extended to support various types of elections like local, state, national, or organizational without major modifications, ensuring long-term usefulness and adaptability.

[7] Limitations

1. Dependence on Stable Internet Connectivity

The proposed blockchain-based voting system requires voters to have a reliable internet connection for interacting with the blockchain (e.g., MetaMask transactions). In regions with poor or unstable internet access, this could restrict participation which is an issue also noted in blockchain e-voting literature, which emphasizes connectivity as a practical challenge for real-world deployment.

2. Blockchain Resource Intensity & Gas Fees

While the prototype uses Ganache with no transaction costs, deploying on a real public blockchain (such as Ethereum) would require paying gas fees, which can fluctuate significantly and increase voting costs. Prior studies highlight resource intensity and performance constraints as ongoing challenges in blockchain e-voting systems, particularly in large-scale elections.

3. Scalability and Performance Constraints

Many current blockchain e-voting solutions, including those reviewed in recent surveys, still face scalability concerns when handling millions of transactions simultaneously. These systems can experience bottlenecks due to consensus overhead and limited transaction throughput, which may affect performance in national-level elections.

4. User Familiarity with Blockchain Tools

The use of tools like MetaMask, wallets, and smart contract interaction may be unfamiliar to some voters particularly those without prior exposure. Research on blockchain e-voting calls attention to usability challenges, which can hinder adoption among non-technical populations.

5. Prototype Tested Only on a Local Blockchain

The system's current evaluation is limited to a local test environment (Ganache). Real deployment on public or consortium blockchains can expose **network, security, and performance issues** that were not observed in the test setup which is a limitation noted by other researchers working on blockchain voting systems.

6. Legal and Regulatory Uncertainties

While not a technical limitation, the broader adoption of blockchain voting systems globally is constrained by political, legal, and regulatory concerns something highlighted in surveys of blockchain e-voting systems, which note that technology readiness does not always align with legislative acceptance.

[8] Future Scope

The proposed blockchain-based NRI voting system has the potential to evolve into a large-scale, nationally deployable voting infrastructure. Numerous other improvements needs to be incorporated in the future:

1. Biometric & Aadhaar-Based Authentication

User Authentication using Biometric verification along with the Aadhaar UID for the authentication and elimination of imitation of identity.

2. Public Blockchain Deployment

This NRI-voting system is currently designed and test on local private blockchain network, but at large scale utilization it has to upgraded and deployed on public blockchain network.

3. AI-Based Fraud Detection

Machine learning models can be added to analyse:

- Detecting malicious patterns in voting
- Multiple attempts to login
- Abnormal transaction thwarts

4. Multi-Language and Voice-Assisted Interface

To access this system in a friendly nature, the User interface needs to be designed in various Indian Regional Languages along with voice-assistance module.

5. Large-Scale National Deployment (Future Use in India)

Even though we have currently developed the model specifically for NRI Voters, but in future the prototype will be utilized at larger scale to handle:

- Local region wise voter of India
- Voters in rural area and at remote distances
- Voters with mobility limitations
- Inter-state migrant workers.

6. Integration with Government Databases

The system can later connect with:

- Election Commission of India (ECI) voter database
- DigiLocker for document verification
- Secure government clouds

This would support real-world deployment with high voter accuracy.

7. Mobile App Version

Developing a dedicated secure mobile application would improve accessibility, allowing voters to authenticate, vote, and track verification all from their smartphones.

[9] Figures and Tables

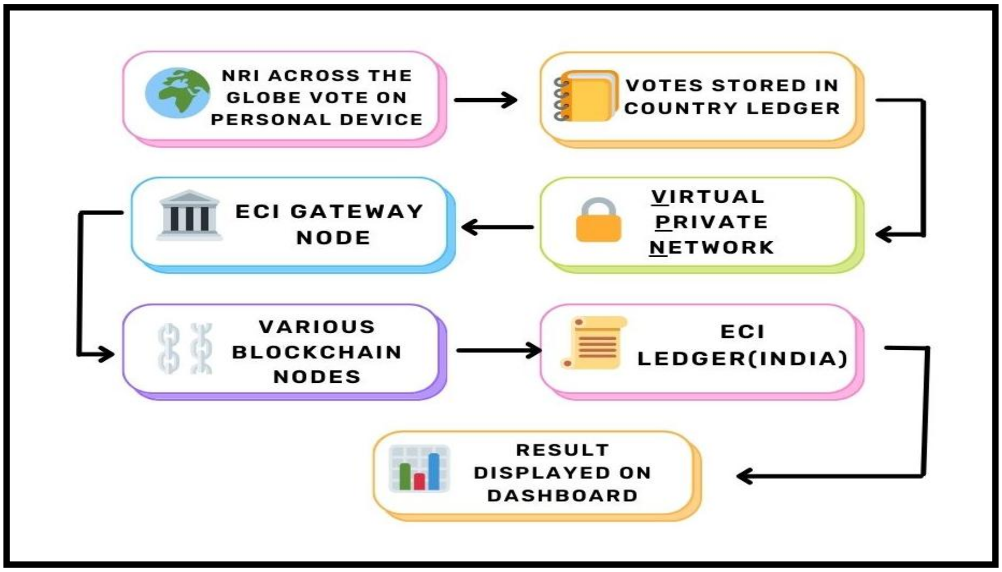

Fig. 1: Flow chart of the System

Table 1: Comparison of Existing Blockchain-Based Electronic Voting Systems

Papers	Technology Used	Authentication Method	Key features	Identified Limitations
[1]	Blockchain, smart contracts	Aadhaar-based verification	Secure voter enrolment, decentralized vote storage, tamper resistance	Limited evaluation in real-world election settings
[2]	Blockchain	Aadhaar credentials	Reduced voter impersonation, improved vote integrity	Scalability and usability aspects not extensively analysed
[3]	Blockchain, IPFS	Biometric authentication	Decentralized storage, enhanced privacy, transparency	Prototype-level implementation without large-scale testing
[4]	Blockchain, IPFS, PBFT	Digital identity mechanisms	Fault tolerance, reliable vote recording, consensus-based validation	Focus primarily on urban election scenarios

[5]	Blockchain, smart contracts	System-based authentication	Automated vote casting and tallying, reduced human intervention	Limited discussion on voter privacy protection
[6]	Survey of blockchain models	Not applicable	Comparative analysis of existing e-voting systems	No practical implementation proposed
[7]	Blockchain review	Not applicable	Identification of security and privacy challenges	Lack of experimental validation

[10] Conclusion

This paper presented a blockchain-based voting framework that makes use of decentralized ledger technology to provide secure, transparent, and tamper-resistant vote recording. By leveraging the immutability of blockchain, the system ensures that votes can be verified by authorized authorities while preventing unauthorized changes, thereby strengthening trust in the overall voting process.

The proposed system specifically addresses the challenges faced by Non-Resident Indian (NRI) voters, such as postal delays, logistical difficulties, and the need for long-distance travel. The integration of smart contracts, MetaMask-based interaction, and secure identity verification demonstrates the practical feasibility of implementing a remote voting solution using blockchain technology.

Although the current prototype is designed with NRI voters in mind, the underlying architecture allows for scalability and future expansion. With suitable policy support and infrastructure, the system can be extended to state-level or national elections in India. The outcomes of this study highlight the role of blockchain as a viable tool for improving transparency and participation in democratic processes, and provide a base for further research and development in digital voting systems.

[11] References

1. Cabuk, U. C., Adiguzel, E., & Karaarslan, E. (2020). A survey on feasibility and suitability of blockchain techniques for e-voting systems. Symmetry, 12(8), 1328.
2. Kumar, R., Gupta, S., & Sharma, A. (2020). A survey of blockchain-based e-voting systems. ResearchGate.
3. Nandimath, P., & Mandape, S. (2023). Blockchain-based secure e-voting system using Aadhaar authentication (Conference paper). IEEE Xplore.
4. Reddy, R., Prasad, K., & Rao, M. (2024). A secure blockchain-based e-voting system using Aadhaar verification. Chitransh Academic Journal.
5. Sahasra, S., Kiran, N., & Ramesh, P. (2023). Smart contract-based e-voting system for secure and transparent elections. Chitransh Academic Journal.
6. Sujatha, K., Divya, P., & Ramesh, S. (2024). Blockchain-powered e-voting system with biometric authentication and IPFS storage. In Proceedings of the International Conference on Cognitive Computing and Cyber Physical Systems (pp. 123–134). Springer.
7. University of Airlangga. (2021). Blockchain-based electronic voting system: Design and analysis (Master’s thesis). Universitas Airlangga Repository.
8. Wang, B., Guo, F., Liu, Y., & Chen, X. (2024). An efficient and versatile e-voting scheme on blockchain. Cybersecurity, 7, Article 62.