A Secure Ethereum-Based Decentralized Voting System Integrating Biometric Authentication and OTP Verification

Gursharanpreet Singh[1], Narinder Singh[2], Er. Rohit Kumar[3], Anchal Singh[4]
[1,2]*Students, B.TECH CSE, SOET, CT University, India*
[3,4]*Assistant Professor, B.TECH CSE, SOET, CT University, India*

Abstract: In the face of technological advancement and greater digital participation, traditional voting has been deemed inefficient, insecure, and opaque. Such problems exist in most democracies, including India, which requires highly dependable, transparent, scalable, and secure systems for managing elections. To address such issues, this article proposes an India-dedicated "Decentralized Voting System" based on "Ethereum Blockchain Technology." This system is a decentralized electronic voting platform that utilizes the intelligence of Ethereum, which offers better security and prevents outside tampering. The system is composed of three distinct solid components: voter registration, voting, and voting outcomes. Each is fortified with advanced cryptography techniques along with "validation through Aadhaar" to guarantee identity while maintaining accessibility. Each component forms the architecture of the system and combines voter registration, voting, and voting outcomes. Due to the structure of Ethereum, fraud, vote tampering, and system manipulation are greatly reduced because of decentralization, transparency, and immutability. Compared to other traditional voting systems, our system has enhanced security, protection, and trust among voters; effectiveness; and expansion capabilities. This implies that our system has the potential to support secure and democratic elections for large populations.

Keywords: Decentralized voting, Ethereum-based blockchain algorithm, online voting, Aadhar-based authentication, and electoral transparency are the keywords.

1. INTRODUCTION

A democratic state incorporates voting as the hallmark of a society, granting citizens the ability to partake in choosing and influencing the government's direction. This process requires reliability, public assurance, safety, trust, and transparency. Over the last few decades, there has been a continuous change in the manner elections are held. The change from manual to electronic voting is one such achievement that aimed to enhance speed, accuracy, security, transparency, and turnout. Expansion of e-voting systems has certain advantages but also poses some significant problems of trust, privacy, and security.

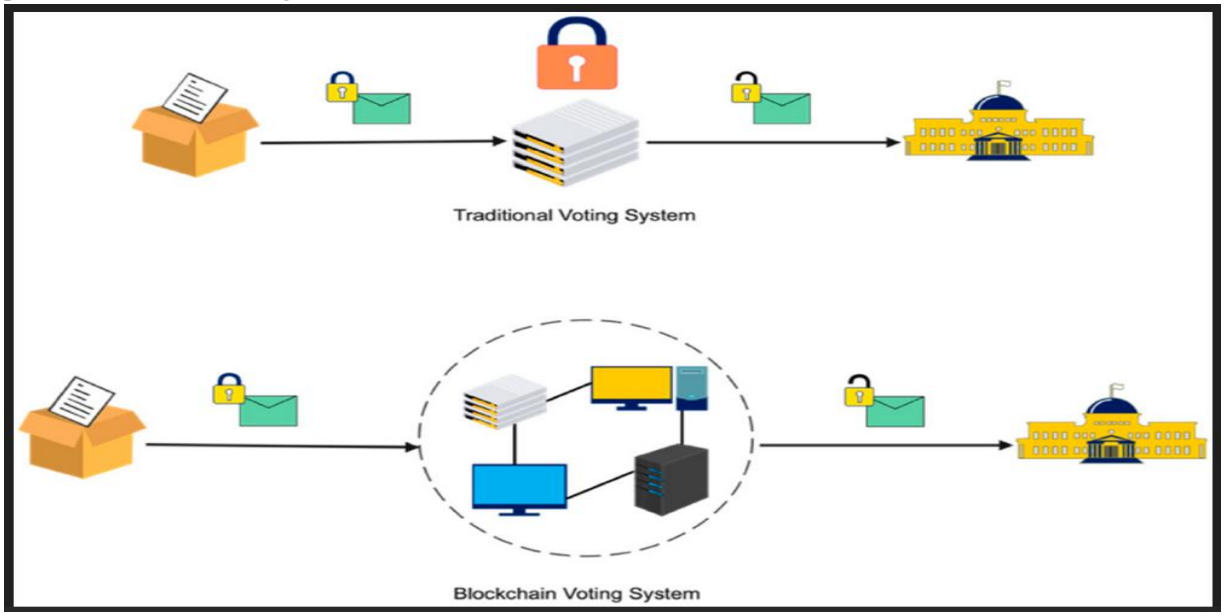

Figure 1.1: Traditional Voting System vs. Blockchain-Based voting system

Blockchain has emerged as a powerful tool enabling secure and difficult-to-alter networks or systems. Blockchain is a distributed ledger kept by multiple participants over a network. The data is stored in blocks that contain cryptographic hashes linking them together. Tampering with the data added to this chain without being detected is borderline impossible. This makes the blockchain liability-free and a lot more appealing for businesses that need care when dealing with sensitive data. The research explores the implementation of a voting system built on the Livelihood Project blockchain, also referred to as Ethereum. Ethereum is one of the most popular blockchains because of its programmable smart contracts. These contracts can automatically execute the voting logic, like verifying voters, distributing tokens, and counting votes. They do not require a central authority. Along with self-executing commands, more trust is integrated in the process because there is no chance for forgery and alteration after editing is set in stone. Ethereum supports transparent elections that can be accessed by any constituent for validation without breaching their privacy because the files are encrypted. Our proposed system tackles the issues of fraud and confidentiality. Each vote can only be recorded once, allowing only a single entry without concealment, eliminating the possibility of multiple false votes.

2. LITERATURE REVIEW

As civic systems continue to adopt advanced technologies, the creation of reliable, easy-to-use, and verifiable voting systems has emerged as an urgent need in democratic societies. Although outdated, the systems used to conduct elections are under intense scrutiny for their inefficiency, vulnerability to fraudulent activities, and centralized control. In this regard, blockchain technology worldwide is considered a revolutionary technology.

2.1 Blockchain-Based Voting System:

In e-voting, the applications of blockchain focused on improving the voting process and eliminating tampering through data immutability. These avoided single points of failure through time-stamped signature cryptographic hashing and smart contracts. This work assisted in the advancement of the development of processes for decentralized voting. Smart contracts have also enhanced the programmable logic on voting systems, making Ethereum a widely used blockchain platform. It enables the automation of democratic processes such as the registration, verification, and counting of votes. This automation lessens human intervention and improves transparency. There is, however, the downside of losing voter privacy due to Ethereum's public access. There is a need to incorporate additional cryptographic measures to mitigate this challenge.

2.2 Privacy-Preserving Voting Protocols:

Researchers now often use privacy-enhancing tools like zero-knowledge proofs (ZKPs) in their work. ZKPs allow voters to show they are eligible and have cast their vote without sharing personal details or the vote itself. This keeps things private even in open systems. In 2024, El Kafhali and their team used "Paillier homomorphic encryption" along with "ZKPs" to keep votes secret along with making audits possible. These kinds of cryptographic methods play a big role in public blockchains like Ethereum, where keeping data open needs to go hand-in-hand with protecting anonymity.

2.3 Biometric and Multimodal Authentication:

Authentication is of utmost importance in the domain of e-voting systems. Some researchers have focused on strengthening security by connecting the voter's biological data to their identity. Hanchinal et al. (2024) applied facial recognition using Local Binary Patterns (LBP) and trained various machine learning classifiers, which achieved identity verification. Simultaneously, systems such as those defended by Sreenivasa et al. (2023) used biometric Aadhaar-linked verification of fingerprints and facial images to authenticate voters with high precision. Often these systems operate using multiple layers of protocols that incorporate OTP verification, ID cards, and biometric scans to the system, which minimizes spoofing or identity-fraud.

2.4 Comparative Analysis:

Table: Comparative analysis of previous work

S. No.	Author & Citation	Conference/ Journal	Algorithm	Challenges

1.	Ms. Kavya Ramesh Naidu, Mr. Ankush Dinesh Ingale, and others et al. (2023)	IRJMETS Journal	Timestamp-based authentication, Elliptic Curve Digital Signature Algorithm, Hybrid Block Chain	1. Ensuring authentication and Eligibility verification. 2. Preventing vote tampering. Avoiding centralized control Vulnerabilities. 3. Hacking and security breaches in the absence of Blockchain.
2.	Noor Ahmed and Prof. Anupama Pattanasetty et al. (2024)	JSRT Journal	Holomorphic Encryption, Chain Security Algorithm, Smart Contracts for secure vote casting	1. Lack of transparency 2. Preventing vote duplication and data manipulation. 3. Protecting voter identities in a public blockchain network. 4. Ensuring real-time tamper-resistance during the voting Process.
3.	Tainiyat K Hanchinal, Vaishali D. Bhavani, Abhilasha Jayakkanavar et al. (2024)	Journal of Current Research in Engineering and Science	LBPH (Local Binary Pattern Histogram) for facial recognition, Machine Learning Classifiers, OTP-based Two-Factor Authentication	1. Accuracy and reliability of facial recognition models. 2. Handling voter identity fraud. 3. Detecting anomalies during voting. 4. Addressing data privacy concerns with facial and biometric data.
4.	Said El Kafhali et al. (2024)	Hindawi Journal	SHA-1/SHA-2, Paillier Homomorphic Encryption, Zero-Knowledge Proofs (ZKP)	1. Scalability of Ethereum for national Level elections. 2. Maintaining vote privacy. 3. High cost of smart contract execution On public blockchains.
5.	N. Sreenivasa, Gopal Agarwal, Rishab Jain et al. (2023)	ITM Web of Conferences	Face Recognition Algorithms, Aadhar-Based Verification, Voter ID Validation, Cryptographic Hashing for vote validation	1. Ensuring accuracy and speed in facial, Aadhar, and voter ID Verifications. 2. Managing multi-step authentication latency. 3. Preventing unauthorized access or Data mismatch across databases. 4. Maintaining system availability and Consistency under load.
6.	Gowtham R, Harsha K N, Manjunatha B, Girish H S, Nithya Kumari R et al. (2019)	IJERT Journal	RFID-Based Voter Verification, OTP Authentication, Biometric (Fingerprint) Authentication, IoT Server-Based Validation	1. Preventing fraud through biometric Spoofing or ID misuse. 2. Integrating IoT securely in real-time Systems. 3. Verifying that a person votes only Once.
7.	Anne-Marie Oostveen & Peter van den Besselaar et al. (2003)	EMTEL Conference,	PKI (Public Key Infrastructure), Secure Internet Voting Protocols	1. Trust in new technologies among Different social groups. 2. Lack of large-scale empirical Validation. 3. Usability and acceptance of online Voting interfaces.
8.	Sanjay Kumar, Dr. Ekta Walia et al. (2011)	IJCSE Conference	No specific algorithm implementation; Discusses security limitations and need for reliable authentication	1. Authentication of users in EVMs. 2. Securing the voting process from Tampering and threats.

2.5 Research Gap:

- Inability to Access on a National Level: Most systems, such as RFID-based, biometric, and Arduino-based systems, are only confined to constituency or district-level voting infrastructure, restricting access for citizens who have nominated or relocated temporarily or on a permanent basis.
- Centralized Databases Are Vulnerable to Alteration: Several approaches depend on centralized databases, such as for the storage of biometrics data or vote which pose danger for

altering security, such as data tampering, breach, or single failure points.

- Count Votes with Manual and Prone to Mistakes: Other systems like Arduino-based or fingerprint voting still have manual supervision when it comes to counting votes, which can lead to errors caused by humans.
- Inactive Procedures for Confirming the Identity of the Voter: Procedures for confirming the identity of the voter established face recognition systems and OTP are scant, skeptical, and with no defense against impersonation traps or interceptions.

3. RESEARCH DESIGN & METHODOLOGY

3.1 Statement of the Research Problem:

Countries like India face challenges in securing and making the voting process more accessible. This problem propounds as developments in electronic voting systems are made; many come with problems such as voter impersonation, limited access for citizens away from their constituencies, data being manipulated from centralized storage, and inefficiency in remote verification. The cost of deploying physical infrastructure for a vast population expands the problem even more. Particular concern is faced by working professionals, students, military personnel, the differently abled, and other active posters who are eligible voters, as they cannot be physically present in their regions on Election Day. Their trust is also broken without manual vote counting being transparent, which makes them question the integrity of the system, coupled with birth capturing, vote tampering, and manual vote counting blunders. Biometric identification systems alongside digital ones do exist, yet most still operate under a vulnerable and dangerously central command style. The system most certainly would be open to attack by some lower administrator or armed attacker. Therefore, the need for amazement, trust, and simple operation increases significantly to let citizens vote from anywhere in the country without needing to verify their claim.

3.2 Objectives:

- Create an immutable, secure, and unchangeable digital voting system on the Ethereum blockchain that guarantees proper recording and preservation of each vote's integrity.
- Encourage citizens unable to return to their home constituencies due to work, study, health, and other service commitments to participate in remote voting from anywhere in the country.
  By implementing a voting system based on blockchain technology, which decentralizes the entire process, the dependency on a centralized system is removed as voting data is stored in the form of blockchain.
- Only eligible persons can access the voting system and cast a vote using secure Aadhaar-linked biometric verification, which strengthens voter authentication.
- Vote counting and result generation will be done by automated processes through the smart contracts that were created for this purpose.
- Develop a graphical user interface that enables participation in the voting activity without prior guidance or training, regardless of one's technical skills and knowledge.

3.3 Methodology:

The following is the procedure we followed in developing a decentralized voting system: we analyzed current systems which are integrated with blockchain. After analyzing the existing systems and processes, we designed an outline that addresses the gaps that were identified.

A step within the methodology was creating a private Ethereum test network. This environment controls voter engagements within a controlled setting. Using Remix and Truffle, smart contracts were built in Solidity for voter registration, vote casting, and result tallying within that environment. Fingerprint hashes alongside Aadhaar-linked unique IDs were held securely and cross-checked at the login stage. Voting was only possible after successful validation was completed. Each vote is considered as a transaction on the Ethereum blockchain. Privacy of voters was guaranteed through encryption techniques that protected individual choices while still allowing the outcomes to be publicly verified. "Web3.js," along with "Metamask," created real-time communication with the smart contract layer and enabled voter interaction through backend blockchain services. A number of test cases were performed to analyze system behavior, including but not limited to vote manipulation and attempts at illegal redundant access. Such tests proved that our system is robust while strengthening the logic of the smart contract.

3.4 Smart Contract Design and Implementation:
A smart contract-based voting system is integrated at the core of the Ethereum ecosystem, which aims to be decentralized. Voters are registered, and votes are cast and recorded all within the same smart contract, which enforces rules like one-person-one-vote and

```
mapping(address => bool) public hasVoted;

function castVote(uint _candidateId) public {
    require(!hasVoted[msg.sender], "Already voted");
    // store encrypted vote
    encryptedVotes[msg.sender] = encryptVote(_candidateId);
    hasVoted[msg.sender] = true;
}
```

Vote Encryption and Privacy: Encryption Technique AES is used to encrypt votes before submission, and here Ethereum serves as a host server, meaning it is a public call. Only hash references that have been anonymized will be stored on-chain. Officials can only decrypt the files once the elections are closed, which means voter anonymity can be guaranteed.

Measures for Edge Cases: The safeguards are used within contracts that resist repetition, restriction of votes during certain circumstances, and invalid candidates. Certain restrictions that cannot be exceeded are enforced, like no submissions can be made post a specific date.

```
require(block.timestamp <= votingDeadline, "Voting period ended");
require(validCandidate(_candidateId), "Invalid candidate");
```

To conclude, an adequate level of security is maintained while preserving modularity and system monitoring, enabling the practical application of the system in real-world voting scenarios with optimized agility for future adjustments.

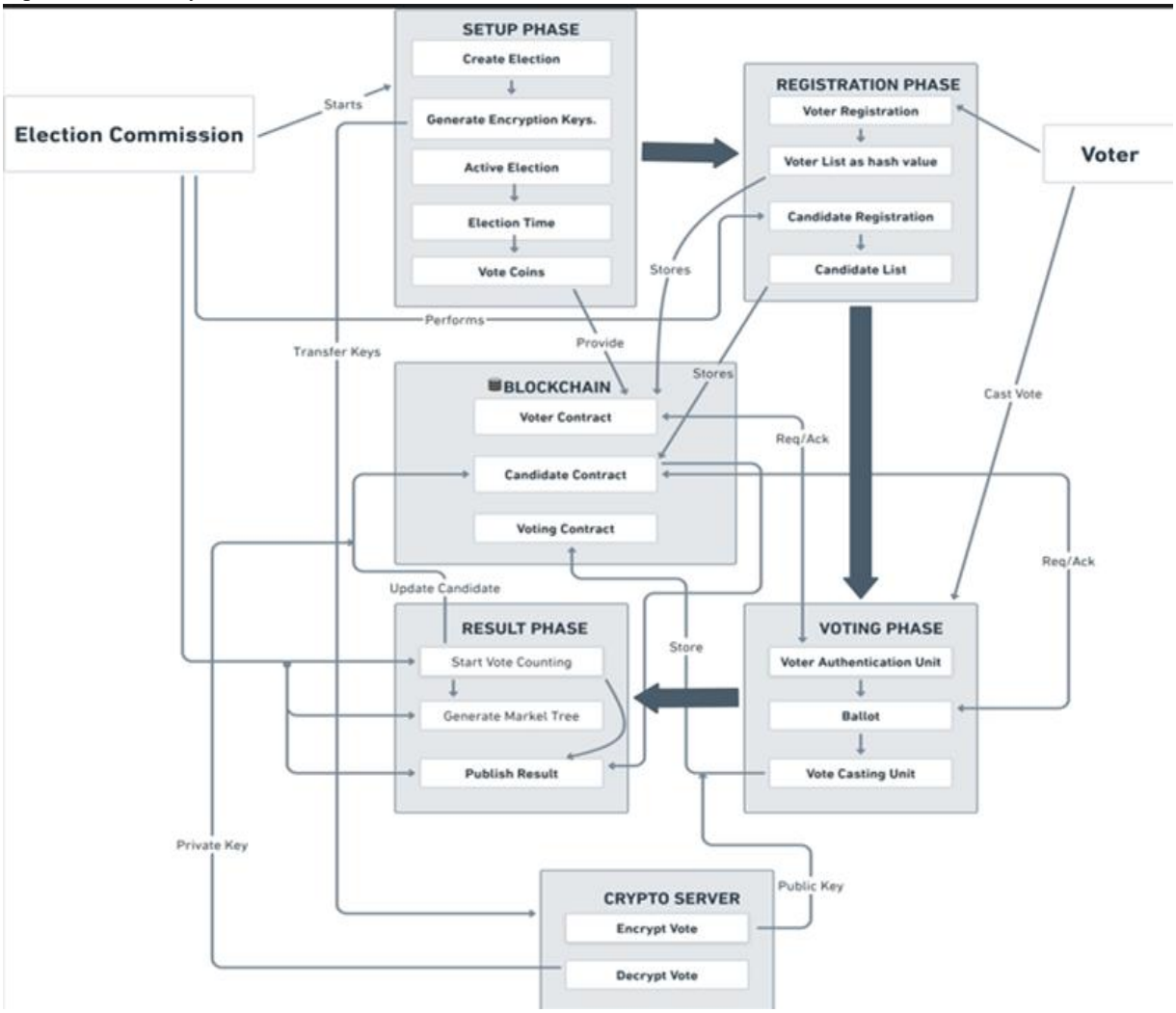

Figure 3.4: Workflow of Block-Chain based Decentralized Voting System. Reprinted from[14].

In the described voting system, users can vote using their smartphones and other smart gadgets. Individuals without smartphones can still vote at a designated voting center. Both online and offline voters follow the same procedure and guidelines set for participatory voting. (See Fig. 3.5.)

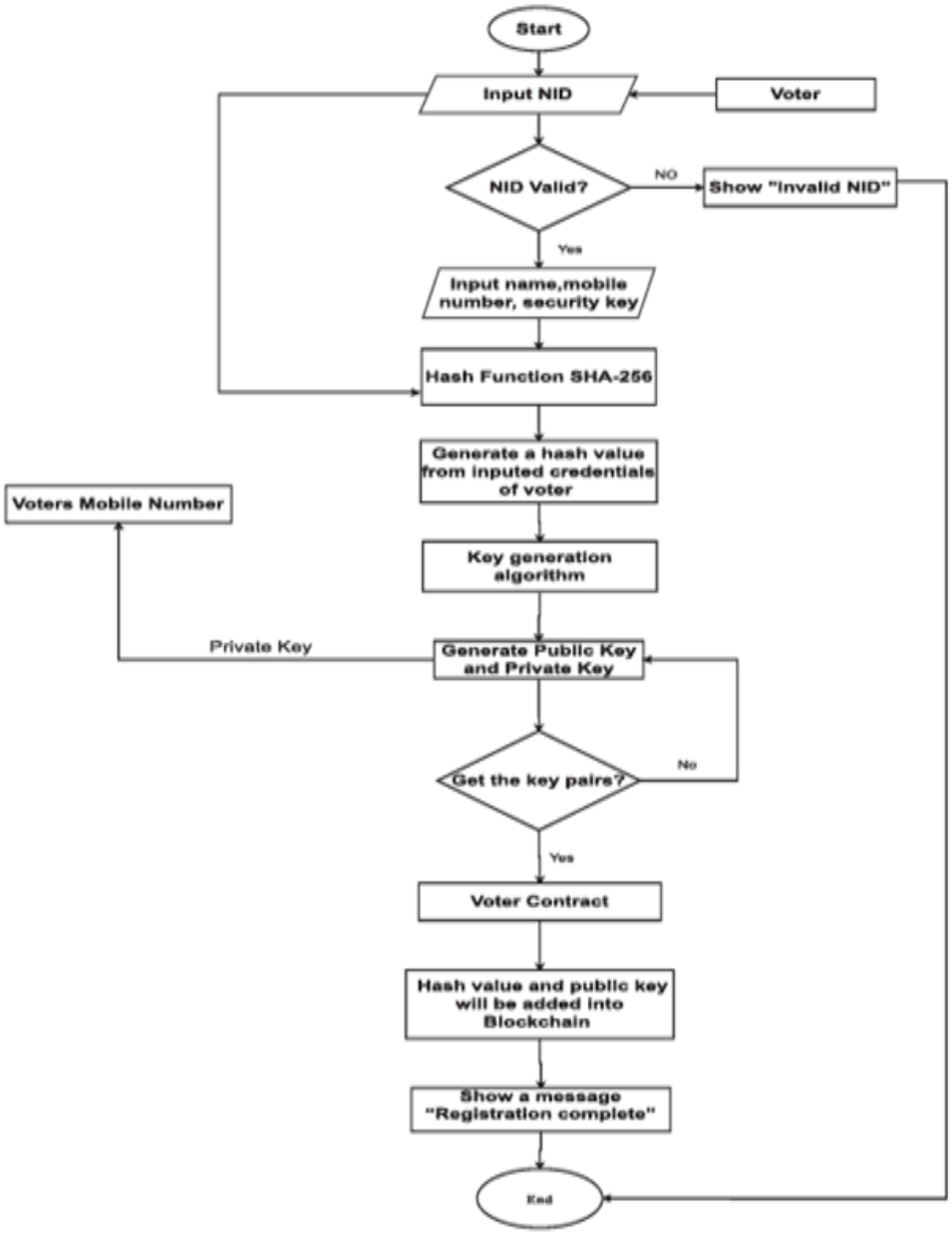

Figure 3.5: Workflow of Voter Registration. Reprinted from [14].

4. RESULT ANALYSIS

The proposed blockchain voting system was successfully implemented and tested on Ethereum's blockchain infrastructure, which gives high accuracy, security, and efficiency in dealing with digital votes. The contracts performed consistently across multiple testing rounds, confirming both the functional stability and the correctness of vote transactions.

One of the key findings from the trial runs was the system's ability to eliminate fake voting attempts. When a user tried to vote a second time using the same biometric ID, the system automatically rejected the request without disrupting the rest of the process. Smart contracts executed this logic with accuracy, and each attempt was permanently recorded on the blockchain, ensuring transparency and accountability. Fig. 4.1 describes a typical voting cycle on the Ethereum network, highlighting each step from biometric verification to the final transaction confirmation.

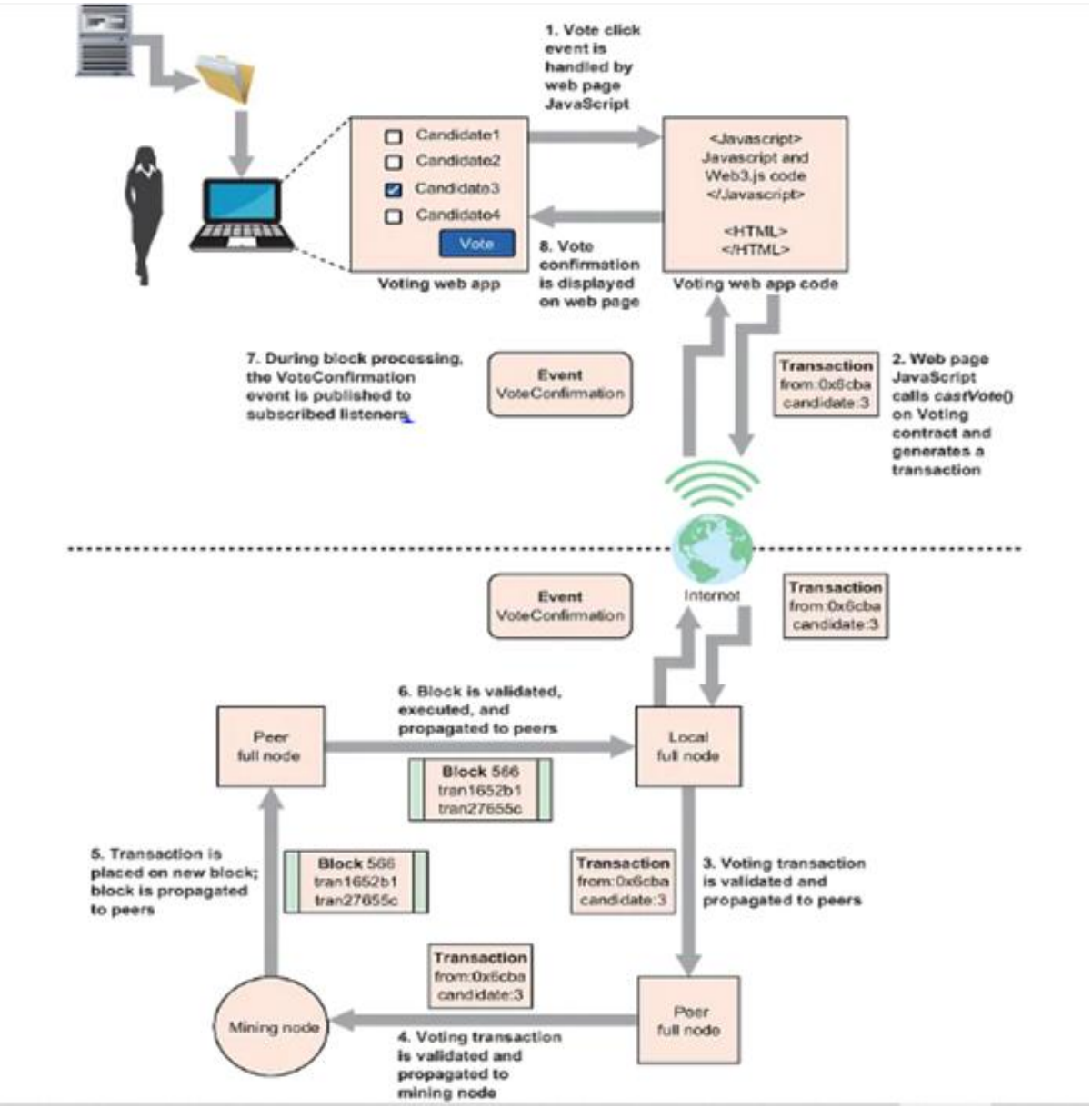

Figure 4.1: Workflow of Voting Cycle on Ethereum Network

The centralized databases, which often experience performance limitations under high load, and the decentralized model showed consistent response times, even when a number of voters cast their votes simultaneously. Security audits revealed strong resistance to common attacks such as double voting, vote manipulation, and unauthorized access. Voter identity was preserved throughout. Since each vote was recorded as a transaction that was encrypted without revealing personal information, privacy was maintained without sacrificing anything. A user-friendly voting interface was also created and tested on multiple devices, including old smartphones, new smartphones, and public desktops. (See Fig. 4.2.)

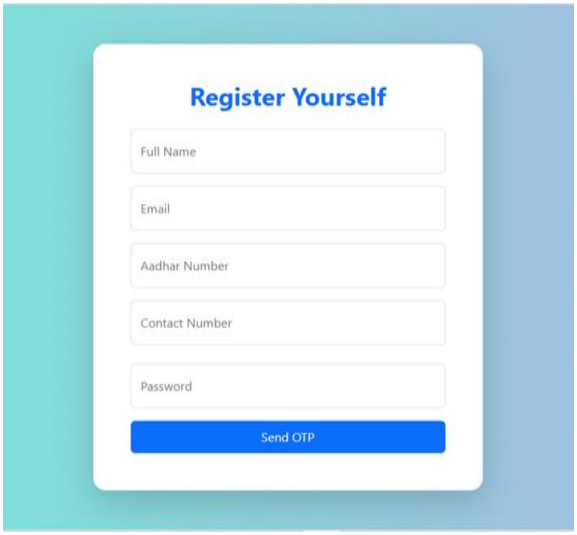

Figure 4.2: Registration Interface.

In conclusion, the performance of the decentralized voting system was high in the areas of privacy, security, speed, and transparency. In contrast to traditional voting systems, the blockchain-based approach not only minimized the possibility of electoral fraud but also ensured that votes were counted accurately and efficiently. Its seamless functionality under substantial stress and extensive usage corroborates its promise in practical applications within democratic systems.

4.1 Quantitative Performance Analysis:

- Gas Fees: While testing the Ethereum Rinkeby test network, each vote as a smart contract function call incurred an average gas fee between 42,000 and 52,000 gas units, contingent on network activity and the complexity of the contract. Using common gas prices (30–50 gwei) and Ethereum costs (~$1,800–2,000/ETH at the time of testing), the expenditure per vote on a public network was estimated to be between $0.70 and $1.20. This indicates that gas costs, albeit reasonable for small-scale elections, would require optimization strategies like batching transactions for efficient execution at the national level.
- Throughput: The system's throughput was found to be in the range of 18 to 22 votes per second (vps), which is an average level of system activity. Such output is primarily determined by Ethereum's block time, which ranges from approximately 13 to 15 seconds. While these figures are not as good for perfectly accommodating local elections or smaller populations, performance may be further improved by using more advanced scalable networks.
- Vote confirmation latency: During the testing, the time taken from submitting the vote to confirming it on the blockchain scope was 16-19 seconds. This time was taken for biometric verification, smart contract execution, and block inclusion. Such delays may not seem bothersome for asynchronous processes like elections, but in real-time voting scenarios, these delays may require voters to wait for extended periods and can be improved via caching, and along with that, we can also perform prioritization at the network to reduce this time of execution.

These observations affirm that while the proposed system performs reliably in controlled environments, its nationwide deployment would require architectural enhancements—such as Layer-2 adoption, parallel contract execution, or migration to a high-throughput blockchain (e.g., Solana, Avalanche).

4.2 Security and Privacy Considerations:

Main Security Challenges and Solutions:

- Sybil Attacks: Aadhaar-linked biometric verification, like fingerprint scans, can prevent impersonation. Enforcement of an ID-based smart contract guarantees one vote per ID.
- Replay Attacks: Votes being counted only once are safeguarded by unique nonces and timestamps, ensuring that each transaction contributes an immutable vote during the voting process.
- Biometric Spoofing: Multimodal verification such as fingerprint and Aadhaar along with OTP, prevents impersonation. Plans of applying liveness verification will increasingly strengthen the system later.

Privacy Improvement:

- It is possible to replace the contents of the vote with pseudonyms Zk-SNARKs without revealing the voter's ID, enabling proving of the contents of the vote for anonymity.
- Voter identity may be hidden while signing within a group, hence anonymously identifying contacts and voters' rings.
- Data Encryption: Metadata tracking will be blocked due to the encryption and anonymization of the votes, which would be stored on-chain.

5. CONCLUSION

The decentralized voting system built using Ethereum performed well in terms of speed, security, privacy, and transparency. The blockchain-based decentralized voting system lowers the possibility of electoral fraud in comparison to existing voting systems, and it also provides effectiveness in vote-counting process. Its potential for practical implementation in democratic processes is confirmed by its ability to function smoothly under high load conditions.

REFERENCES

[1] Kavya Ramesh Naidu, Ankush Dinesh Ingale, Pratiksha Sukhadeo Gaikwad, Hitesh Rajendra Thakare, Sujal Sunil Chavan, and Yogeshk Sharma, "Online Voting System," *International Research Journal of Modernization in Engineering, Technology and Science*, vol. 5, no. 5, May 2023. Available: https://www.doi.org/10.56726/IRJMETS38984

[2] Beulah Jayakumari, S. Lilly Sheeba, Maya Eapen, Jani Anbarasi, Vinayakumar Ravi, A. Suganya, and Malathy Jawahar, "E-voting system using cloud-based hybrid blockchain technology," *Journal of Safety Science and Resilience*, vol. 5, pp. 102–109, 2024. Available: https://doi.org/10.1016/j.jnlssr.2024.01.002

[3] Kashif Mehboob Khan, Junaid Arshad, and Muhammad Mubashir Khan, "Secure Digital Voting System Based on Blockchain Technology," *NED University of Engineering and Technology, Pakistan; University of West London, UK.* Available: https://core.ac.uk/display/155779036

[4] Tainiyat K. Hanchinal, Vaishali D. Bhavani, and Abhilasha Jayakkanavar, "Online Voting System Based on Machine Learning," *International Journal of Emerging Trends in Research*, vol. 7, no. 2, Jan. 2024.

[5] Sanjay Kumar and Ekta Walia, "Analysis of Electronic Voting System in Various Countries," *International Journal on Computer Science and Engineering (IJCSE)*, May 2011. Available: https://www.researchgate.net/publication/267235287

[6] N. Sreenivasa, Gopal Agarwal, and Rishab Jain, "Online Voting System by Using Three-Step Verification," *ITM Web of Conferences*, vol. 57, paper 01010, ICAECT 2023. Available:https://doi.org/10.1051/itmconf/20235701010

[7] Said El Kafhali, "Blockchain-Based Electronic Voting System: Significance and Requirements," *Mathematical Problems in Engineering*, vol. 2024, Article ID 5591147, 2024. Available: https://doi.org/10.1155/2024/5591147

[8] Noor Ahmed and Anupama Pattanasetty, "Online Voting Using Blockchain," *Journal of Scientific Research and Technology (JSRT)*, vol. 2, no. 3, Mar. 2024. Available: www.jsrtjournal.com

[9] Anne-Marie Oostveen and Peter van den Besselaar, "E-voting and Media Effects: An Exploratory Study," *EMTEL Conference*, London, Apr. 2003. Available: https://www.researchgate.net/publication/267235287

[10] Gowtham R., Harsha K. N., Manjunatha B., Girish H. S., and Nithya Kumari R., "Smart Voting System," *International Journal of Engineering Research & Technology (IJERT)*, vol. 8, issue 4, Apr. 2020. Available: https://www.ijert.org/smart-voting-system

[11] Prof. Anisaara Nadaph, Rakhi Bondre, Ashmita Katiyar, Durgesh Goswami, and Tushar Naidu, "An Implementation of Secure Online Voting System," International Journal of Engineering Research and General Science, vol. 3, no. 2, Mar.–Apr. 2015.

[12] K. P. Kaliyamurthie, R. Udayakumar, D. Parameswari, and S. N. Mugunthan, "Highly Secured Online Voting System over Network," Indian Journal of Science and Technology, vol. 6, no. 6S, May 2013.

[13] Smita Khairnar and Reena Kharat, "Survey on Secure Online Voting System," International Journal of Computer Applications, vol. 134, no. 13, Jan. 2016.

[14] Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, and Sajib Ahamed, "DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system," *Journal of King Saud University – Computer and Information Sciences*, vol. 34, pp. 6855–6871, 2022. https://doi.org/10.1016/j.jksuci.2022.06.014