Online Voting System Using Blockchain: A Comprehensive Approach

Ameya Mane, Atharva Birje, Harsh Minde, Jyotiraditya Patil

Abstract: In recent years, blockchain technology has gained significant traction as a robust solution to address the challenges of traditional voting systems such as fraud, tampering, inefficiency, and high operational costs. This paper presents the design and development of a blockchain-based online voting system aimed at revolutionizing electoral processes in large democracies like India. The system utilizes the Ethereum blockchain to securely record votes in an immutable and decentralized manner while integrating secondary database to manage metadata and alot, reducing the load on the blockchain to ensure scalability and performance.

The proposed solution, developed as an mobile application, offers multi-factor authentication (MFA) for voter security, real-time election results, and comprehensive election classifications. By minimizing human intervention and leveraging the decentralized nature of blockchain, this system aims to replace existing manual and electronic voting methods, providing a cost-effective, transparent, and efficient alternative. Key features include vote validation, real-time result visualization in various formats, and the ability to handle large-scale elections with reduced resource consumption. The system also incorporates risk mitigation strategies to safeguard voter privacy and ensure data integrity throughout the election process.

1. Introduction:

1.1. Background

India, the world's largest democracy, conducts elections on an enormous scale involving millions of voters across geographically and socially diverse regions. Traditional voting systems, reliant on manual processes and Electronic Voting Machines (EVMs), are often subject to inefficiencies, fraud, tampering, requiring vast resources in terms of manpower and finances. These challenges undermine public trust in the electoral process, delay result declaration, and inflate operational costs. Blockchain technology, with its decentralized and immutable characteristics, has emerged as a robust solution to enhance security, transparency, and efficiency in voting systems. By ensuring that each vote is securely stored and tamper-proof, blockchain can significantly reduce the vulnerabilities of traditional methods.

1.2. Objectives

The primary objective of this project is to develop a secure, scalable, and efficient blockchain-based voting system that can address key challenges such as voter fraud, vote tampering, and inefficiencies in traditional voting processes. The system leverages Ethereum's immutable ledger for vote recording and employs secondary database for managing non-voting-related metadata, thereby reducing the operational burden on the blockchain and minimizing transaction costs. With features like multi-factor authentication (MFA), real-time result visualization, and enhanced voter privacy, the system is designed to handle large-scale elections in India, offering a cost-effective, transparent, and secure alternative to current voting methods.

2. Related Work:

2.1 Traditional Voting Systems

Current voting systems, such as paper ballots and Electronic Voting Machines (EVMs), are widely used in countries like India. While effective to an extent, they come with several challenges: vulnerability to tampering, reliance on centralized databases, and a need for extensive manpower, which results in high operational costs. Additionally, these systems often face delays in result declaration and the potential for data breaches or manipulation within centralized systems remains a concern.

2.2 Blockchain-Based Voting Solutions

Blockchain technology has been proposed as a solution to the issues faced by traditional voting systems. Several studies have explored the security advantages of decentralized tamper-proof records of votes through blockchain. By leveraging blockchain's decentralized nature, these systems ensure that once a vote is recorded, it cannot be altered, thereby enhancing voter trust and system transparency. However, blockchain voting systems also face challenges. One major issue is scalability, especially when dealing with elections on the scale of those in India, which involves a massive number of voters and high transaction volumes.

Our proposed system builds on hybrid approach by using blockchain for vote storage and validation, while handling metadata & other activities & operations through Secondary database, ensuring a scalable and cost-effective solution for large-scale elections. Additionally, our system incorporates real-time election results, multifactor authentication (MFA), and region-wise classifications of voters and results, addressing both performance and security concerns highlighted in previous studies.

3. Problem Statement:

India's existing electoral systems, despite advancements like the use of Electronic Voting Machines (EVMs), are still vulnerable to tampering, inefficiencies, and high operational costs. The current voting process demands substantial resources in terms of manpower, time, and infrastructure, leading to delays and the potential for fraud or errors. These centralized systems also introduce security vulnerabilities, as the reliance on manual oversight and centralized databases leaves the election process open to manipulation.

The need for a decentralized, secure, and scalable solution is paramount, especially in a country with a population as large and diverse as India. This project aims to address these issues by developing a blockchain-based voting system. By leveraging blockchain's inherent transparency and immutability, the proposed system ensures the integrity of votes while reducing the dependency on traditional EVMs and manual processes. Furthermore, to handle large-scale elections efficiently, Firebase will be integrated to manage metadata, reducing transaction loads and operational costs on the blockchain.

4. Literature Review:

4.1 Traditional Voting Methods

Traditional voting methods, such as Electronic Voting Machines (EVMs) and paper ballots, have long been the backbone of democratic elections. However, several studies have highlighted their limitations. These methods are vulnerable to tampering, manipulation, and often require significant resources to ensure accuracy. Centralized databases used in traditional voting systems can be compromised, leading to potential election rigging and manipulation. Additionally, they are prone to delays in result declaration, causing inefficiencies in the voting process.
Previous research underscores the need for a decentralized and tamper-proof voting solution that can reduce the reliance on centralized databases while ensuring transparency and trust. This sets the stage for exploring blockchain as a transformative technology in modern voting systems.

4.2 Blockchain in Voting Systems

Blockchain technology has garnered significant interest in recent years due to its potential to create secure, transparent, and decentralized voting systems. Several studies highlight how blockchain can address key challenges in traditional voting, such as data integrity, transparency, and security.

Blockchain Enabled Online-Voting System (2020) and **A Scalable Implementation of Anonymous Voting over Ethereum Blockchain (2021)**:

- These studies emphasize the benefits of blockchain in building tamper-proof, transparent voting mechanisms. The decentralized nature of blockchain ensures that no single entity can alter election results.
- Blockchain ensures the immutability of votes, meaning once a vote is cast, it cannot be modified or deleted, thus eliminating the risks of tampering.
- Smart contracts on Ethereum blockchain are used to automate the validation and counting of votes. However, one major limitation remains scalability, as large-scale elections, such as national elections, often overwhelm blockchain networks.
- Our project builds on these works by introducing a hybrid solution that combines the strengths of blockchain with off-chain storage systems like Firebase. This integration helps reduce blockchain load and transaction costs, improving scalability for large-scale elections like those in India.

4.3 Mobile Voting Platforms

Mobile voting systems are becoming increasingly important due to the widespread adoption of smartphones. Research on mobile voting platforms highlights their potential to make voting more accessible and user-friendly.

Paper 4 (Android-Based Voting Application):

- This paper discusses the convenience of using mobile applications for voting, offering a familiar interface for users.
- Mobile platforms allow users to participate in multiple elections from the same app, providing a seamless experience.
- By incorporating security features like multifactor authentication (MFA) and biometric verification, mobile voting systems can ensure that only eligible voters can access and cast votes.

Our project leverages this research by designing a **Flutter-based mobile app** that simplifies the voting process, enabling voter registration, vote casting, and real-time election result display. The app integrates biometric authentication and MFA to ensure security and voter integrity.

4.4 Smart Contracts for Election Management

Smart contracts are essential to automating the election process on a blockchain. Several studies have explored their use in managing key functions such as vote validation, counting, and result declaration.

Paper 3 (Smart Contracts for Election Management):

- This research outlines the use of smart contracts in elections to enforce predefined rules, such as ensuring one vote per voter and preventing double voting.
- Smart contracts also automate the process of counting votes and announcing results, significantly reducing human errors and delays.

Our system implements Ethereum-based **smart contracts** that validate and securely store each vote. The contracts also count votes in real time, ensuring transparency and prompt result announcement once voting concludes.

4.5 Security Measures in E-Voting Systems

Security is one of the most critical aspects of any voting system. Several papers focus on methods to enhance the security of e-voting systems using techniques such as encryption, multifactor authentication, and audit trails.

Paper 5 (Security in E-Voting Systems):

- This paper explores how MFA and encryption techniques can be integrated into voting systems to ensure that only authorized individuals can cast votes.
- Additionally, the paper discusses the importance of maintaining audit logs to track suspicious activities while preserving voter anonymity.

Our system incorporates **end-to-end encryption** to secure data transmitted between the mobile app, backend, and blockchain. **MFA and biometric verification** ensure that only eligible voters can participate in the election, and audit logs are maintained in Firebase to provide transparency and traceability without compromising voter privacy.

4.6 Scalability Challenges in Blockchain Voting Systems

Scalability remains a significant challenge for blockchain-based voting systems, particularly when used in large-scale elections.

Paper 6 (Scalability of Blockchain Voting Systems):

- This paper addresses the scalability limitations of blockchain, especially in high-load scenarios such as national elections. The high transaction costs and potential delays are significant barriers to adoption.
- The paper suggests exploring hybrid solutions that leverage off-chain storage for non-sensitive data to reduce blockchain congestion.

Our system integrates **Firebase** as an off-chain database to store non-vote-related data, such as voter metadata and logs. This reduces the transaction load on the blockchain, allowing it to handle only critical operations related to vote storage, ensuring efficient performance during peak voting periods.

This literature review synthesizes key insights from academic research on blockchain-based voting systems, mobile voting platforms, and smart contracts. By combining these elements, our proposed system offers a **secure, scalable, and transparent** voting solution that leverages blockchain for vote storage and validation while using Firebase for non-sensitive data. This hybrid approach addresses the challenges of traditional voting systems, ensuring integrity, accessibility, and efficiency, particularly in large-scale elections.

5. Proposed Solution:

5.1. Technical Design

5.1.1. Data Flow and System Components

5.1.2. Scalability and Security

5.1.3. System Components and Integration

5.2. System Architecture

5.2.1. The proposed system consists of three key components:

1. **Mobile Application (UI):**
   Developed in Android Studio using Kotlin or Flutter, this mobile app provides an intuitive interface for voters. It allows users to:
   - register securely using multi-factor authentication (MFA), including biometric verification and OTPs.
   - Users can browse available elections, view candidates, and cast votes in a user-friendly environment.
   - Access to real-time election results is presented in both textual and graphical formats.

2. **Blockchain Integration:**
   The Ethereum blockchain will be used to record votes as immutable transactions. Key functions include:
   - smart contracts (developed in Solidity) that handle vote validation, counting, and enforce one-vote-per-user rules.
   - Immutable storage of votes and election results, ensuring tamper-proof records.

3. **Secondary Database:**
   To reduce the load and transaction costs on the blockchain, Firebase will manage non-sensitive data such as:
   - Voter profiles
   - Election metadata (e.g., election dates, candidate lists)
   - Logs and audit trails for system operations

   This hybrid architecture offloads non-critical data from the blockchain while maintaining the integrity and scalability needed for large elections.

5.2.2. Voting Process

5.2.3. Key Features

5.3. Technical Components:

5.3.1. User Interface (UI)

5.3.2. Backend System (Node.js)

5.3.3. Blockchain Integration (Ethereum)

5.3.4. Firebase for Metadata Management

This solution offers a secure, decentralized, and scalable voting system designed to address the current inefficiencies in India's traditional electoral processes. By integrating blockchain for vote security and Secondary database for managing non-sensitive metadata, the system is designed to handle large-scale elections efficiently, reducing costs and ensuring voter trust.

This technical design ensures a **secure, scalable, and efficient voting system** capable of handling large-scale elections, such as those in India. The hybrid architecture optimizes the strengths of blockchain technology while leveraging Firebase to reduce costs and enhance performance.

6. Methodology

The system integrates **Ganache/Truffle**, **Ethereum**, and **Secondary Database** to create a secure, scalable, and efficient voting platform. Below is a breakdown of how the system components interact and function:

6.1 Blockchain Integration

6.1.1 Development Environment:

1. **Ganache/Truffle:**
   During the development phase, Ganache and Truffle will be used to simulate a local Ethereum blockchain environment. This will enable testing of smart contracts and voting transactions in a controlled setup before deploying to the live Ethereum network.

2. **Web3.js and Node.js:**
   These tools will facilitate communication between the mobile app, backend, and blockchain. Web3.js will handle smart contract interactions from the frontend, while Node.js will manage API requests and backend operations.

6.1.2 Voting Process:

1. **Vote Transactions:**
   Once a voter casts a vote, the mobile app sends the transaction to the backend. The backend then interacts with the Ethereum blockchain using smart contracts to record each vote as a transaction.

2. **Vote Validation:**
   Smart contracts written in Solidity will validate each vote, ensuring authenticity and preventing multiple votes from the same voter.

3. **Result Publication:**
   As soon as voting is concluded, smart contracts automatically count votes and publish results in real-time on the blockchain, providing transparency and immutability.

6.2 Security and Privacy

6.2.1 Multi-factor Authentication (MFA):

The system will incorporate MFA, including biometric or OTP-based authentication, to ensure that only legitimate users can vote.

6.2.2 End-to-End Encryption:

All data transmitted between the mobile app, backend, and blockchain is encrypted to protect user privacy and system security.

6.2.3 Anonymity and Transparency:

1. **Blockchain Ledger:**
   While the blockchain maintains a transparent ledger of transactions (votes), the anonymity of each vote is preserved, ensuring voter privacy.

2. **Smart Contracts for Security:**
   Smart contracts ensure that each vote is unique, correctly counted, and tamper-proof.

6.3 Performance Optimization

6.3.1 Data Segmentation:

1. **Blockchain for Votes:**
   Only sensitive data, such as votes and election results, are stored on the Ethereum blockchain to leverage its immutability and security features.

2. **Firebase for Non-sensitive Data:**
   Non-vote-related data, such as voter profiles, election metadata, and user activity logs, will be stored in **Firebase**. This approach reduces the load on the blockchain and ensures faster system performance, particularly during peak voting times.

6.3.2 Cost-Effectiveness:

1. **Transaction Batching:**
   To minimize gas fees and improve performance, vote transactions are batched together during high voting volumes.

2. **Optimized Scalability:**
   By offloading non-critical data to Firebase, the system remains scalable and cost-effective during large-scale elections, such as national elections.

6.4 Process Breakdown

6.4.1 Voter Registration:

1. **User Flow:**

Users register through the mobile app by providing identification details, which are verified through MFA. Once verified, the system generates a unique voter ID, which is stored on the blockchain for future voting authentication.

6.4.2 Vote Casting:

1. **User Flow:**
   After selecting a candidate from the list of eligible elections, the vote is securely transmitted to the Ethereum blockchain via the backend. A confirmation message is displayed in the app once the vote is successfully recorded on the blockchain.

2. **Transaction Validation:**
   Smart contracts verify the legitimacy of the vote and ensure that no voter casts more than one vote.

6.4.3 Data Handling and Storage:

1. **Sensitive Data:**
   Votes are stored immutably on the blockchain, ensuring that they cannot be altered or tampered with once submitted.

2. **Non-Sensitive Data**
   Voter profiles, election logs, and other non-critical information are stored in Firebase, optimizing the system's speed and reducing blockchain congestion.

6.4.4 Result Display:

1. **Real-Time Updates:**
   Once voting is complete, the system uses smart contracts to process and count votes. The results are automatically updated and displayed in real-time through the mobile app, with both list and graphical formats available for users.

2. **Transparency:**
   Since votes are recorded on the blockchain, the result calculation process is transparent and auditable, enhancing the election's credibility.

6.5 Security Measures

6.5.1 End-to-End Encryption:

All communications between the app, backend, and blockchain are encrypted to prevent unauthorized data interception.

6.5.2 Smart Contracts for Security:

Solidity-based smart contracts manage vote validation, counting, and result declaration, ensuring accuracy and security.

6.5.3 MFA & Biometrics:

Multi-factor authentication and optional biometric login provide additional layers of security, preventing unauthorized access to the voting system.

Blockchain-Based Voting Security:
The system draws on research, such as the secure electronic voting systems outlined [2], which emphasize the use of blockchain and mobile technologies for privacy and security in elections.

Scalability Insights:
The system's architecture takes lessons [16], which addresses scalability challenges in blockchain-based applications, ensuring that the voting system can handle high voter turnout without compromising performance.

The methodology combines cutting-edge blockchain technology, a secure backend, and optimized data handling using Firebase to build a robust, scalable, and secure online voting system. The use of smart contracts, MFA, and real-time results ensures the system’s transparency and trustworthiness, while performance optimizations make it feasible for large-scale elections globally.

7 Challenges and Solutions:

7.1 Blockchain Scalability

Challenge:

Public blockchains like Ethereum, while highly secure and decentralized, face scalability limitations. During large-scale elections, the sheer volume of transactions can lead to network congestion, increased transaction times, and higher costs due to fluctuating gas fees.

Solution:

1. **Layer 2 Scaling Solutions:**
   The integration of Layer 2 protocols (e.g., rollups or sidechains) allows for faster and cheaper transactions by processing them off-chain before settling them on the main Ethereum chain. This ensures that high voter turnout can be handled without overwhelming the network.

2. **Private Blockchain Option:**
   As an alternative, a private or permissioned blockchain could be considered. Private blockchains offer greater control over transaction throughput and cost, making them ideal for large, national elections that need high transaction capacity.

3. **Transaction Batching:**
   Instead of submitting each vote individually, transactions are grouped into batches and processed together. This reduces the number of interactions with the blockchain and helps to optimize performance, particularly during peak voting periods.

7.2 Security Threats

Challenge:

The system is vulnerable to various cybersecurity threats, including Distributed Denial-of-Service (DDoS) attacks, unauthorized access, and data breaches. Ensuring that the system remains secure from such attacks is critical for maintaining voter trust and election integrity.

Solution:

1. **Strong Encryption:**
   End-to-end encryption is applied to all communications between the mobile app, backend, and blockchain to ensure that sensitive data remains secure during transmission.

2. **Multi-Factor Authentication (MFA):**
   MFA, which includes biometric authentication (fingerprint, facial recognition) and OTPs, is enforced to protect voter accounts and prevent unauthorized access to the system.

3. **Rate Limiting & DDoS Protection:**
   The system employs rate limiting on API calls and backend functions to protect against DDoS attacks. Regular penetration testing and security audits further ensure the robustness of the system against external threats.

4. **Smart Contract Audits:**
   All smart contracts are rigorously audited to prevent vulnerabilities and ensure they execute voting processes securely.

7.3 User Privacy

Challenge:

Maintaining voter privacy is essential, especially in an electronic voting system. Sensitive data, such as voter identities and votes, must be protected, and the anonymity of votes should be guaranteed without compromising the integrity of the election.

Solution:

1. **Data Segregation:**
   The system isolates sensitive vote data on the blockchain, which provides tamper-proof storage and ensures anonymity. Meanwhile, non-sensitive data, such as voter profiles, election metadata, and activity logs, are stored in Firebase to optimize performance and reduce blockchain costs.

2. **Data Encryption:**
   All voter information, including non-sensitive data stored in Firebase, is encrypted at rest and in transit to ensure that no unauthorized entity can access or tamper with it.

3. **Audit Logs:**
   The system generates comprehensive audit logs that election officials can use to verify the integrity of the election without compromising the privacy of individual voters.

By addressing the challenges of **scalability**, **security**, and **user privacy**, the **Online Voting System Using Blockchain** can provide a reliable, secure, and efficient platform capable of handling large-scale elections, such as those in India, while maintaining voter trust and election transparency.

8. Risk Management and Mitigation:

8.1 Scalability Issues

Ethereum's limited transaction throughput may cause delays during high-volume elections, especially in a populous country like India. To mitigate this, the system will utilize **Layer 2 scaling solutions**, such as rollups, and implement **transaction batching** to improve performance and reduce congestion. Non-essential data will be offloaded to Firebase, ensuring smooth operation even during peak voting times.

8.2 Data Privacy Concerns

Storing sensitive voting data on a public blockchain raises privacy concerns. To address this, the system isolates sensitive data (votes) on the blockchain and ensures that only non-sensitive metadata, such as logs and voter participation, is handled by Firebase. **End-to-end encryption** is applied to all data transmissions, ensuring that both blockchain-stored votes and Firebase metadata are secure. Privacy measures such as **homomorphic encryption** or **zero-knowledge proofs** may also be explored in future iterations.

8.3 Security Threats

To protect the system from Distributed Denial-of-Service (DDoS) attacks and other security threats, **rate limiting**, **firewalls**, and **multi-factor authentication (MFA)** are implemented at the backend level. Biometric authentication adds an extra layer of security, preventing unauthorized access. Regular **security audits** and **monitoring** are carried out to identify and address potential vulnerabilities.

8.4 System Downtime

To ensure the system's availability during high-traffic periods, **backup servers**, **load balancing**, and **failover mechanisms** are put in place. Continuous performance monitoring ensures that the system remains operational and any issues are addressed in real time.

By implementing these mitigation strategies, the system is equipped to handle scalability, privacy, security, and operational risks effectively.

9. Results and Evaluation:

10. Expected Outcome

The **Online Voting System Using Blockchain** is expected to deliver the following key outcomes:

10.1 Secure Voting Process:

10.1.1 Immutable Vote Recording:

Votes cast through the mobile app will be stored immutably on the Ethereum blockchain, ensuring that they cannot be tampered with or altered after submission. This guarantees the integrity of the voting process.

10.2 Real-Time Results:

10.2.1 Transparency and Speed:

The system will display election results in real-time, with both textual and graphical representations of the number of votes each candidate has received. This feature will enhance transparency, allowing both voters and election officials to monitor results as they are tallied.

10.3 Auditability:

10.3.1 Comprehensive Election Logs:

Election-related data, such as voter participation, metadata, and activity logs, will be stored in Firebase, enabling election officials and auditors to review the process without compromising voter anonymity. This ensures a transparent and auditable electoral process.

10.4 Cost Efficiency:

10.4.1 Reduction of Election Costs:

By leveraging blockchain technology and reducing the need for physical voting machinery like Electronic Voting Machines (EVMs), the system significantly cuts costs associated with running elections. Additionally, it minimizes manpower requirements, making it more cost-effective for large-scale national elections.

10.5 Scalability and Performance:

10.5.1 Handling Large Voter Bases:

The system is designed to handle high user loads during peak election periods, such as national elections. The use of transaction batching and offloading non-sensitive data to Firebase ensures that the blockchain remains scalable and efficient.

10.6 Enhanced Security:

10.6.1 Multi-Factor Authentication (MFA):

The system ensures that only verified voters can access the platform and cast votes, adding an extra layer of security to prevent unauthorized access.

10.6.2 End-to-End Encryption:

All communications between the mobile app, backend, and blockchain are encrypted, further enhancing the security of voter data and the election process.

10.7 User Engagement and Voter Participation:

10.7.1 Participation Tracking:

The system provides features that allow election officials to track voter participation in real-time. This information can be used to improve voter turnout and identify patterns in voter behavior.

The system is expected to deliver a secure, transparent, and cost-effective solution for conducting elections, capable of scaling for both local and national elections in India and globally. By leveraging blockchain technology for vote storage and using Firebase for additional data management, the system ensures performance, security, and transparency while maintaining voter privacy.

11. Conclusion

This paper presents a blockchain-based online voting system designed to improve the security, transparency, and efficiency of elections, particularly in large-scale scenarios like those in India. By integrating Ethereum's blockchain technology with Firebase, the system provides a scalable, tamper-proof, and cost-effective solution for conducting elections. Blockchain ensures that votes are recorded immutably, preventing fraud and vote tampering, while Firebase handles non-sensitive data, optimizing system performance and reducing costs.

The proposed system addresses key challenges such as scalability through transaction batching and Layer 2 solutions, and it enhances security by implementing end-to-end encryption, multi-factor authentication, and audit logs. With real-time results and auditability, the system boosts transparency, helping to foster voter trust and ensuring election integrity.

By reducing reliance on manual processes and traditional voting machines, this blockchain-based system represents a transformative step towards modernizing elections, offering a viable solution for secure, scalable, and efficient democratic processes.

12. Future Work

Future enhancements of the proposed blockchain-based online voting system can focus on several key areas to improve scalability, privacy, and functionality:

1. **International Expansion**: The system can be adapted for use in international elections, addressing the specific requirements of different countries and regions.
2. **Enhanced Privacy**: Advanced encryption techniques, such as homomorphic encryption or zero-knowledge proofs, can be explored to further protect voter privacy while maintaining transparency.
3. **Layer-2 Scaling**: Further exploration of Layer-2 solutions like rollups or sidechains could help improve transaction throughput, making the system more efficient for large-scale elections.
4. **Biometric Security**: Additional biometric authentication methods, such as facial recognition or voice biometrics, can be integrated to enhance security.
5. **Artificial Intelligence and Machine Learning**: AI/ML can be utilized to detect voting patterns, analyze voter behavior, and predict election outcomes. This would provide valuable insights to election authorities for better decision-making and improving voter engagement.

By pursuing these directions, the system can become more robust, secure, and scalable for global adoption.

References

1. "Blockchain Enabled Online-Voting System." *ITM Web of Conferences*, 2020.
2. "A Scalable Implementation of Anonymous Voting over Ethereum Blockchain." *IEEE Access*, 2021.
3. "Implementation of Decentralized Blockchain E-voting." *International Journal of Computer Applications*, 2018.
4. "Decentralized Voting Platform Based on Ethereum Blockchain." *International Conference on Decentralized Applications and Infrastructures*, 2020.