A SYNOPSIS ON

BLOCKCHAIN-ENVISIONED VOTING SYSTEM

Submitted in partial fulfillment of the requirement for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

Submitted by:

Student Name	University Roll No.
Sarthak Singh Rawat	2019078
Rajeev Sharma	2019031
Brian J Peter	2018766
Shivansh Dharni	2019108

Under the Guidance of

Dr. Mohammad Wazid
Professor, Department of
Computer Science and Engineering

Project Team ID. – MP24CSE056

Department of Computer Science and Engineering
Graphic Era (Deemed to be University)
Dehradun, Uttarakhand

October-2024

CANDIDATE'S DECLARATION

We hereby certify that the work which is being presented in the Synopsis entitled "Blockchain-envisioned Voting System" in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering in the Department of Computer Science and Engineering of the Graphic Era (Deemed to be University), Dehradun shall be carried out by the undersigned under the supervision of **Dr. Mohammad Wazid**, Professor, Department of Computer Science and Engineering, Graphic Era (Deemed to be University), Dehradun.

Name	**University Roll.No**	**Signature**
Rajeev Sharma	2019031	
Sarthak Singh Rawat	2019078	
Brian J Peter	2018766	
Shivansh Dharni	2019108	

The above mentioned students shall be working under the supervision of the undersigned on the "Blockchain-envisioned Voting System".

Signature
Supervisor

Signature
Head of the Department

Internal Evaluation (By DPRC Committee)

Status of the Synopsis: Accepted / Rejected

Any Comments :

Name of the Committee Members: **Signature with Date**

1.

2.

Table of Contents

Chapter 1

Introduction

1.1 Introduction

In an era of rapid technological advancement, the fundamental processes of democracy are ripe for innovation. The voting system, a cornerstone of democratic societies, has long been plagued by issues of security, transparency, and accessibility. As we progress further into the digital age, the need for a more robust, efficient, and trustworthy voting mechanism has become increasingly apparent. Enter blockchain technology – a revolutionary approach to data management that promises to address many of the shortcomings of traditional voting systems.

1.1.1 The Current State of Voting Systems

Traditional voting systems, whether paper-based or electronic, face numerous challenges:
1. Lack of Transparency: Limited ability for voters to verify that their votes were correctly recorded and counted.
2. Accessibility Issues: Difficulty in accommodating remote voters or those with physical limitations.
3. Cost and Efficiency: High expenses associated with organizing and managing elections, including personnel, equipment, and security measures.
4. Voter Turnout: Inconvenience and logistical hurdles that may discourage participation.

These issues have led to decreased public trust in electoral processes and, in some cases, disputed election results. The need for a more secure, transparent, and accessible voting system has never been more critical.

1.1.2 Blockchain Technology

Blockchain technology, originally developed as the underlying mechanism for cryptocurrencies like Bitcoin, has shown tremendous potential in various fields beyond finance. At its core, blockchain is a distributed ledger technology that allows for secure, transparent, and immutable record-keeping.
Key features of blockchain that make it suitable for voting systems include:

i. **Decentralization**: No single point of failure or control, making the system resistant to manipulation.
ii. **Transparency**: All transactions (votes) are visible to all participants, ensuring openness.
iii. **Immutability**: Once recorded, data cannot be altered without consensus from the network.
iv. **Security**: Cryptographic techniques ensure the integrity and authenticity of each transaction.
v. **Auditability**: The entire voting process can be easily verified and audited.

1.1.3 Blockchain-based Voting

A blockchain-based voting system has the potential to revolutionize the electoral process by addressing the shortcomings of traditional systems:

1. Security: The decentralized nature of blockchain makes it extremely difficult for malicious actors to manipulate votes or compromise the system.
2. Increased Transparency: Voters can verify that their votes have been correctly recorded and counted, fostering trust in the electoral process.
3. Improved Accessibility: Remote voting becomes more feasible and secure, potentially increasing voter participation.
4. Cost-Effective: While initial implementation costs may be high, long-term expenses could be significantly reduced by automating many aspects of the voting process.
5. Real-time Results: Vote counting can be done in real-time, providing instant and accurate results.
6. Elimination of Voter Fraud: Blockchain's immutability and the use of cryptographic techniques can prevent double-voting and other forms of electoral fraud.

Therefore, this project aims to design and implement a prototype blockchain-based voting system that addresses the challenges while capitalizing on the technology's strengths.

Chapter 2

Literature Survey

Blockchain technology has emerged as a promising solution to address the numerous challenges faced by traditional electronic voting systems. The inherent properties of blockchain, such as immutability, transparency, and decentralization, make it an attractive option for creating more secure, transparent, and efficient voting systems. This literary survey examines the current state of research on blockchain-based voting systems, exploring various approaches, benefits, challenges, and future directions.

The concept of electronic voting has been around for decades, but it has been plagued by issues related to security, transparency, and voter privacy [1]. Traditional e-voting systems often rely on centralized architectures, making them vulnerable to single points of failure and potential manipulation. Moreover, the lack of transparency in these systems has led to public distrust and concerns about the integrity of election results. Blockchain technology, first introduced as the underlying technology for cryptocurrencies like Bitcoin, has shown potential to address these issues in voting systems [2].

Researchers have proposed several approaches to implementing blockchain-based voting systems. One common approach involves using public blockchain platforms, such as Ethereum, to create decentralized voting applications. McCorry et al. proposed a smart contract-based system for boardroom voting that maximizes voter privacy. Their system leverages the Ethereum blockchain to ensure transparency and immutability of votes while using cryptographic techniques to protect voter anonymity [3]. Similarly, Yavuz et al. developed an Ethereum-based e-voting system that aims to provide a secure and transparent voting process [4].

While public blockchain-based systems offer high levels of transparency and decentralization, they face scalability challenges when dealing with large-scale elections. To address this issue, some researchers have proposed using private or permissioned blockchains. These systems offer better control over access and improved scalability, often using consensus algorithms like Practical Byzantine Fault Tolerance (PBFT) instead of the resource-intensive Proof of Work

used in many public blockchains. Tasca and Tessone provide a comprehensive taxonomy of blockchain technologies, including private and permissioned blockchains, which can be applied to voting systems [5].

Hybrid approaches combining public and private blockchains have also been proposed to balance transparency and scalability. Pawlak et al. suggested a system that uses a private blockchain for vote collection and a public blockchain for result verification. This approach aims to leverage the strengths of both types of blockchains while mitigating their respective weaknesses [6].

The potential benefits of blockchain-based voting systems are numerous. Transparency is perhaps the most significant advantage, as blockchain's immutable ledger provides a clear and auditable record of all transactions. This transparency can greatly enhance trust in the voting process, as noted by Meter in his design of distributed voting systems. The decentralized nature of blockchain also contributes to improved security, making the system resistant to single points of failure and various types of attacks [7]. Atzori explored how blockchain technology and decentralized governance could potentially reshape the role of the state in managing elections [8].

Another key benefit is the potential for enhanced voter privacy. While blockchain transactions are typically public, cryptographic techniques can be employed to ensure voter anonymity while maintaining verifiability. Park et al. discussed various approaches to achieving this balance between privacy and verifiability in blockchain voting systems [9]. Additionally, blockchain-based systems could potentially reduce the long-term costs of elections by eliminating the need for extensive physical infrastructure, as suggested by Akbari et al. [10].

Despite these potential benefits, blockchain-based voting systems face several challenges and limitations. Scalability remains a significant issue, particularly for public blockchain networks. As Wang et al. discussed in their survey of consensus mechanisms, the current throughput of many blockchain networks is insufficient to handle the volume of transactions required for large-scale national elections [11]. Voter authentication is another critical challenge, as ensuring secure and privacy-preserving authentication in a digital environment is complex. Yi

explored various approaches to securing e-voting based on blockchain in P2P networks, highlighting the importance of robust authentication mechanisms [12].

The digital divide presents another obstacle to the widespread adoption of blockchain-based voting systems. As Hjálmarsson et al. pointed out, the technology gap may exclude certain populations from participating in such systems, raising concerns about equity and accessibility. [13]. Furthermore, adapting blockchain-based voting systems to comply with existing election laws and regulations presents significant challenges, as discussed by Hsiao et al. in their work on decentralized e-voting systems [14].

In conclusion, blockchain-based voting systems show significant promise in addressing many of the challenges faced by traditional electronic voting systems. The technology offers potential improvements in transparency, security, and voter privacy. However, substantial research and development are still needed to overcome existing limitations, particularly in areas of scalability, authentication, and regulatory compliance. As the technology continues to evolve and mature, it may play an increasingly important role in shaping the future of democratic processes worldwide.

Chapter 3

Objectives

The Objectives include:

i. Developing a secure and scalable blockchain architecture suitable for large-scale elections.

ii. Implementing robust voter authentication mechanisms to prevent fraud.

iii. Ensuring voter privacy through advanced cryptographic techniques.

iv. Creating a user-friendly interface accessible to voters with varying levels of technical proficiency.

v. Designing a system for real-time vote counting and result verification.

vi. Conducting thorough security audits and stress tests to validate the system's integrity.

Chapter 4

Hardware and Software Requirements

4.1 Hardware Requirements

i. For Local Development:
   a. Processor: Quad-core (i5 or higher recommended)
   b. RAM: 8 GB minimum (16 GB recommended)
   c. Storage: 256 GB SSD minimum (preferably 512 GB or more)
   d. Internet: Stable internet connection for accessing blockchain networks and development tools

ii. For Deployment:
   a. Server: Cloud-based services such as AWS, Azure, or Google Cloud
   b. CPU: 4 vCPUs or higher
   c. RAM: 16 GB or higher
   d. Storage: SSD with 1 TB for database and blockchain logs
   e. Backup: Dedicated backup storage (preferably in the cloud)
   f. Network: High-bandwidth internet connection to handle blockchain interactions and voting activities
   g. Security: Firewalls and encryption-enabled servers

4.2 Software Requirements

i. Blockchain Tools:
   a. Node Version Manager (nvm): To manage Node.js versions
   b. Hardhat Node: For local blockchain simulation
   c. Metamask: Ethereum wallet for connecting to the blockchain network
   d. Hardhat: Framework for smart contract development and testing
   e. Alchemy: To interact with the Ethereum blockchain (Arbitrum Sepolia)
   f. Solidity Compiler: For writing and deploying smart contracts

ii. Programming Languages:
   a. Solidity: For developing smart contracts

b. JavaScript (Node.js): Backend services and API creation
c. PostgreSQL: For database querying
d. Next.js: For building the user interface
e. HTML/CSS: Web page structure and styling

iii. Databases:
a. Supabase Tables: For storing user details (Aadhar number, name, email, etc.)

iv. Development Tools:
a. Visual Studio Code (VSCode): IDE for coding
b. Postman: For testing APIs
c. Git: Version control system
d. Docker (optional): For containerizing the application

v. Security Tools:
a. OpenZeppelin: For secure and reliable smart contract libraries.
b. Ethereum Testnet (Sepolia): For testing transactions before deployment.

vi. Cloud Services:
a. AWS/Azure/Google Cloud: For hosting and scaling the backend services
b. Ethereum node providers (e.g., Infura, Alchemy): For blockchain node management.

vii. Additional Tools:
a. Metamask: Browser extension wallet for interacting with the blockchain
b. Account Abstraction Tools: Framework to abstract away complexities of wallet creation.

These requirements will ensure smooth development, testing, and deployment of your blockchain-based voting system.

Chapter 5

Possible Approach/Algorithms

5.1 System Architecture

The blockchain-based voting system will be built on a three-tier architecture:

- Blockchain Layer (Ethereum - Arbitrum Sepolia L2)
- Backend Layer (Node.js server and Supabase)
- Frontend Layer (NextJs web application)

5.2 Smart Contract Design

The core of the voting system will be implemented as a smart contract on the Arbitrum Sepolia L2 network. Key components include:

i. **1. Admin Management**
   a. Store an array of admin addresses
   b. Implement functions to add/remove admins
   c. Require multi-sig (3/4 agreement) for critical actions

ii. **2. Member Management**
   a. Struct to store member information (address, status)
   b. Mapping of addresses to member structs
   c. Functions for admin approval of new members

iii. **3. Proposal Management**
   a. Struct to store proposal details (description, voting period, status)
   b. Mapping of proposal IDs to proposal structs
   c. Functions for admins to create proposals

iv. **4. Voting Mechanism**

a. Mapping to track votes (proposal ID => address => vote)
b. Functions for members to cast votes
c. Vote counting and proposal status update logic

5.3 Backend Server Design

Supa base will handle user registration, authentication, and NodeJs server will act as an intermediary between the frontend and the blockchain. Key components include:

i. **User Management**

a. API endpoints for user registration and login
b. Validation of Aadhaar numbers, email addresses, and other user data
c. Secure storage of user information in Supabase tables

ii. **Blockchain Interaction**

a. Integration with Ethers.js for smart contract interactions
b. Management of user wallet addresses and transaction signing

iii. **Admin Interface**

a. API endpoints for admins to review and approve new members
b. Synchronization of approved members with the blockchain

References

[1] A. Kiayias and M. Yung, "Self-tallying elections and perfect ballot secrecy," in Public Key Cryptography, Berlin, Heidelberg: Springer, 2010, pp. 141-158.

[2] N. Kshetri and J. Voas, "Blockchain-enabled e-voting," IEEE Software, vol. 35, no. 4, pp. 95-99, 2018.

[3] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in Financial Cryptography and Data Security, Cham: Springer, 2017, pp. 357-375.

[4] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, 2018, pp. 1-7.

[5] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," Ledger, vol. 4, 2019.

[6] M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Procedia Computer Science, vol. 141, pp. 239-246, 2018.

[7] C. Meter, "Design of distributed voting systems," arXiv preprint arXiv:1702.02566, 2017.

[8] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?," Journal of Governance and Regulation, vol. 6, no. 1, pp. 45-62, 2017.

[9] S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: From internet voting to blockchain voting," Journal of Cybersecurity, vol. 7, no. 1, p. tyaa025, 2021.

[10] E. Akbari et al., "From blockchain to internet-based voting," in 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, 2017, pp. 218-221.

[11] W. Wang et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," IEEE Access, vol. 7, pp. 22328-22370, 2019.

[12] H. Yi, "Securing e-voting based on blockchain in P2P network," EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, pp. 1-9, 2019.

[13] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson, "Blockchain-based e-voting system," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986.

[14] J. H. Hsiao, R. Tso, C. M. Chen, and M. E. Wu, "Decentralized e-voting systems based on the blockchain technology," in Advanced Information Networking and Applications Workshops (WAINA), 2017 31st International Conference on, Taipei, 2017, pp. 1-2.