Online Voting System Using Blockchain

Major Project I Report

Submitted in partial fulfillment of the requirements for the degree of

Bachelor of Engineering (Computer Engineering)

by:

1. **Atharva Birje**   **ID No:- TU3F2122158**

2. **Harsh Minde**   **ID No:- TU3F2122164**

3. **Jyotiraditya Patil**   **ID No:- TU3F2122181**

4. **Ameya Mane**   **ID No:- TU3F2122206**

Under the Guidance of
Prof. Dnyaneshwar Thombre.

Department of Computer Engineering

TERNA ENGINEERING COLLEGE

Plot no.12, Sector-22, Opp. Nerul Railway station,

Phase-11, Nerul (W), Navi Mumbai 400706

(University of Mumbai)

(2024-2025)

TERNA ENGINEERING COLLEGE, NERUL,

NAVI MUMBAI

Department of Computer Engineering

Academic Year 2024-25

CERTIFICATE

This is to certify that the major project I entitles **"Online Voting System Using Blockchain"** is a Bonafide work of

1)	**Atharva Birje**	**ID No: TU3F2122158**
2)	**Harsh Minde**	**ID No: TU3F2122164**
3)	**Jyotiraditya Patil**	**ID No: TU3F2122181**
4)	**Ameya Mane**	**ID No: TU3F2122206**

submitted to the University of Mumbai in partial fulfillment of the requirement for the award of the Bachelor of Engineering (Computer Engineering).

Guide   **Head of Department**   **Principal**

Project Report Approval

This Major Project Report – an entitled "**Online Voting System Using Blockchain**" by following students is approved for the degree of *B.E. in "Computer Engineering"*.

Submitted by:

1.	**Atharva Birje**	**ID No: TU3F2122158**
2.	**Harsh Minde**	**ID No: TU3F2122164**
3.	**Jyotiraditya Patil**	**ID No: TU3F2122181**
4.	**Ameya Mane**	**ID No: TU3F2122206**

Examiners Name & Signature:

1.---

2.---

Date: ---------------------------------

Place: ---------------------------------

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Atharva Birje   **ID No: TU3F2122158**

Harsh Minde   **ID No: TU3F2122164**

Jyotiraditya Patil   **ID No: TU3F2122181**

Ameya Mane   **ID No: TU3F2122206**

Date: _____

Place: _____

Acknowledgement

We would like to express our sincere gratitude towards our guide **Prof. Dnyaneshwar Thombre**, Project Coordinator **Dr. Mohini Misale** for their help, guidance and encouragement, they provided during the project development. This work would have not been possible without their valuable time, patience and motivation. We thank them for making my stint thoroughly pleasant and enriching. It was great learning and an honor being their student.

We are deeply thankful to **Dr. Kishor Sakure (H.O.D Computer Department)** and entire team in the Computer Department. They supported us with scientific guidance, advice and encouragement, they were always helpful and enthusiastic and this inspired us in our work.

We take the privilege to express our sincere thanks to **Dr. L. K. Ragha** our Principal for providing the encouragement and much support throughout our work.

1. **Atharva Birje**   **ID No: TU3F2122158**
2. **Harsh Minde**   **ID No: TU3F2122164**
3. **Jyotiraditya Patil**   **ID No: TU3F2122181**
4. **Ameya Mane**   **ID No: TU3F2122206**

Date: _____

Place: _____

<u>INDEX</u>

TABLE OF CONTENTS

Sr. No.	Title	Page No.
	Abstract	7
	List of Figures	8
	List of Tables	8
Chapter 1	Introduction	9
Chapter 2	Problem Statement	11
Chapter 3	Literature Review	14
Chapter 4	Software Analysis	20
Chapter 5	Design & Implementation	24
Chapter 6	Methodology	33
Chapter 7	Conclusion and Future Scope	35
	Reference	36

<u>Abstract</u>

The Online Voting System Using Blockchain aims to modernize voting processes by addressing issues like fraud, tampering, inefficiencies, and high costs. Traditional systems, particularly in large democracies like India, are resource-heavy and vulnerable to manipulation. By using the Ethereum blockchain, this project secures votes in a tamper-proof and auditable manner, ensuring integrity and transparency. To address scalability issues, the system combines blockchain with Firebase for off-chain storage of non-sensitive data, such as voter profiles and election metadata. This hybrid approach reduces the load on the blockchain, enhancing speed and lowering operational costs. Multi-factor authentication (MFA) and biometric verification ensure that only authorized voters can cast their votes, adding another layer of security.

The system features real-time result visualization, showing election progress immediately as votes are recorded on the blockchain. This ensures transparency, providing a region-wise breakdown of results. Voter privacy and anonymity are maintained by storing sensitive data on the blockchain while handling participation metadata off-chain, allowing election officials to verify participation without compromising privacy. This project offers a scalable, secure, and cost-effective alternative to traditional voting systems, significantly reducing reliance on physical infrastructure like Electronic Voting Machines (EVMs). The transparency, real-time results, and auditability make it ideal for large-scale elections in India and other democracies, ensuring a modern, efficient, and tamper-proof voting process.

Chapter 1

Introduction

1.1 Introduction:-

Elections are the cornerstone of democracy, enabling citizens to choose their representatives. In large democracies like India, traditional voting methods, such as paper ballots and Electronic Voting Machines (EVMs), face challenges like voter fraud, tampering, inefficiency, and high costs. The centralized nature of these systems increases their vulnerability to manipulation, threatening the integrity of election results.

Blockchain technology offers a solution through its decentralized, immutable, and transparent features. By recording votes on a tamper-proof ledger, blockchain enhances voter confidence and ensures vote integrity. The system's automation through smart contracts reduces human errors and ensures timely results. This project aims to develop a Blockchain-Based Online Voting System integrated with a mobile voting app to improve accessibility. It addresses scalability by incorporating Firebase to manage non-sensitive data, ensuring performance optimization for large-scale elections.

This project seeks to modernize the electoral process by providing a secure, efficient, and cost-effective alternative to traditional voting systems, particularly relevant for India's vast electoral landscape. The proposed system reduces resources and time while ensuring the integrity of elections from local to national levels.

1.2 <u>Organization</u> <u>of</u> <u>the</u> <u>Report</u>:-

This report is divided into several key chapters:

1. **Introduction:** Discusses the motivation for the project, the limitations of traditional voting systems, and the advantages of blockchain.
2. **Problem Statement:** Identifies the key challenges of existing electoral systems, including fraud, high costs, and inefficiencies, and outlines the objectives of the proposed system.
3. **Literature Review:** Reviews previous works on traditional and blockchain-based voting systems, highlighting the strengths and limitations of existing approaches.
4. **Software Analysis (SA):** Details the functional, performance, and security requirements needed for successful implementation.
5. **Design and Implementation:** Provides an overview of the system's architecture, including diagrams illustrating blockchain integration and backend systems.
6. **Methodology:** Describes the tools, platforms, and processes used for the development of the system.
7. **Conclusion and Future Scope:** Summarizes key findings and discusses potential improvements for future optimization.
8. **References:** Lists all sources cited throughout the project.

This structure guides readers through the development of the blockchain-based online voting system, providing a clear understanding of the project's objectives, methodology, and outcomes.

Chapter 2

Problem Statement

2.1 Problem statement:-

Elections are the foundation of a democratic system, ensuring that citizens have the right to choose their representatives through a free and fair process. In a country as vast as India, where millions of voters participate in elections at various levels (from Gram Panchayat to Lok Sabha), traditional voting methods face significant challenges. These challenges include security vulnerabilities, vote tampering, fraud, and inefficiencies that can compromise the integrity of the electoral process.

Traditional voting systems, including paper ballots and Electronic Voting Machines (EVMs), are susceptible to multiple forms of manipulation and are heavily reliant on manual processes. The centralized nature of these systems increases the risks of data breaches and tampering, with possibilities of unauthorized access, hacking, or altering vote counts. Moreover, the centralized databases used for storing election data are vulnerable to cyberattacks, which can lead to data manipulation or loss. This not only compromises the accuracy of election results but also damages public trust in the entire democratic process.

Another major concern is the scalability and cost associated with conducting elections in a country as populous as India. Managing millions of voters across geographically diverse and socially distinct regions is a highly resource-intensive process, requiring significant manpower, infrastructure, and finances. Additionally, traditional systems often experience delays in result declaration, with the process of counting votes and verifying results being slow and prone to human error.

The need for a secure, transparent, and efficient solution is paramount, particularly in the digital age, where there is an increasing demand for online and mobile-based services. However, online voting systems have their own challenges, primarily related to security and voter privacy. Implementing a decentralized solution like blockchain technology offers the potential to mitigate these issues by ensuring that votes are securely recorded in an immutable, tamper-proof ledger, without the need for a centralized authority.

The current problem therefore lies in addressing the following key issues with traditional voting systems:

1.   Voter fraud and tampering due to centralized databases and manual handling.

2.   Inefficiency and high operational costs of large-scale elections.

3.   Lack of transparency and delays in result declaration.

4.   Voter privacy and data security concerns in online voting systems.

5.   Scalability issues that make existing systems unsuitable for large, diverse populations like India.

To resolve these issues, there is a clear need for a Blockchain-Based Online Voting System that ensures vote integrity, security, privacy, and efficiency, particularly for large-scale elections.

2.2 <u>Objectives</u>:-

The primary objective of this project is to design and implement a Blockchain-Based Online Voting System that addresses the limitations and challenges of traditional voting systems, ensuring that the electoral process is secure, transparent, and scalable. The key objectives are as follows:

1.Secure Vote Storage Using Blockchain: To leverage Ethereum blockchain technology to securely record votes in an immutable and decentralized manner. The blockchain will ensure that once a vote is cast, it cannot be tampered with or altered. By decentralizing vote storage, the system eliminates the vulnerabilities of a centralized database and ensures that votes are permanently secured in a tamper-proof ledger.

2.Voter Authentication and Privacy: To implement Multi-Factor Authentication (MFA) and biometric verification to ensure that only authorized voters can access the voting system. This objective is critical for ensuring the legitimacy of voters and preventing unauthorized access. At the same time, the system must ensure voter privacy by isolating sensitive data and providing anonymity during vote casting.

3.Smart Contract Integration for Vote Validation and Counting: To develop smart contracts that automate the vote validation, counting, and result declaration processes. The smart contracts, deployed on the Ethereum blockchain, will ensure that each voter can only vote once and that votes are counted transparently and automatically. This will reduce the reliance on human intervention and minimize the chances of errors or manipulation during vote counting.

4.Real-Time Result Visualization: To provide real-time election results that can be viewed by voters and election officials through a mobile app. The system will display election results immediately as votes are recorded on the blockchain, offering both list and graphical views. This objective is essential for enhancing the transparency and efficiency of the election process.

5.Scalability and Cost-Effectiveness: To integrate a secondary database (Firebase) to handle non-sensitive data such as voter profiles, logs, and election metadata. This will reduce the load on the blockchain and ensure that the system can scale to handle large numbers of voters during national or regional elections. The hybrid approach will also reduce operational costs associated with blockchain transactions, making the system more cost-effective for large-scale elections.

6.Comprehensive Election Coverage: To support various levels of elections, including Gram Panchayat, Vidhan Sabha, and Lok Sabha elections. The system will allow voters to participate in elections based on their geographic location, offering comprehensive coverage of the entire electoral process.

7.Transparency and Audibility: To ensure that the system provides full transparency in the voting process by maintaining an immutable record of all transactions (votes) on the blockchain. The system must allow for auditability by election officials without compromising voter privacy. This objective is critical to restoring public trust in the electoral process and ensuring that the system remains credible and trustworthy.

8.Future Scalability and Enhancements: To design the system in such a way that it can be further enhanced in the future by incorporating Layer-2 scaling solutions, such as rollups or sidechains, and potentially integrating Artificial Intelligence (AI) for analyzing voter patterns and behaviors. This objective ensures that the system is not only suitable for current use cases but can also adapt to future technological advancements and electoral needs.

Chapter 3

Literature Review

The *Blockchain Enabled Online-Voting System* developed by Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerjee, and Madhuri Chavan (2020) utilizes blockchain to create an immutable and transparent voting system. The project incorporates 128-bit AES encryption and SHA-256 to enhance security, ensuring that the votes cast are secure and tamper-proof. The system employs authentication methods such as unique identification keys and biometric fingerprint verification, ensuring that only authorized voters can participate. Votes are cast and recorded as blockchain transactions, preserving their integrity and transparency throughout the election process. [1]

In their paper *A Privacy-Preserving Voting Protocol on Blockchain*, Wenbin Zhang et al. (2018) introduced a decentralized voting protocol leveraging homomorphic encryption and distributed tallying, effectively removing the need for trusted third parties. The protocol ensures voter privacy by encrypting votes and distributing ballots across peers while also detecting and correcting dishonest votes without compromising anonymity. The system uses Hyperledger Fabric, making it particularly suitable for small to medium-scale elections where privacy is a critical concern. [2]

The paper by Stephan Neumann, Oksana Kulyk, and Melanie Volkamer (2014) describes a *Usable Android Application Implementing Distributed Cryptography* for Election Authorities. This Android app is designed to facilitate secure distributed key generation and verifiable vote decryption for non-technical election authorities. While it simplifies the voting process for non-experts, the authors highlight that users struggled with understanding complex security concepts, suggesting the need for improved educational tools to assist users in navigating cryptographic security. [3]

Jae-Geun Song, Sung-Jun Moon, and Ju-Wook Jang (2021) developed *A Scalable Implementation of Anonymous Voting over Ethereum Blockchain* to address scalability issues in blockchain voting systems. Their implementation successfully scales to accommodate a larger number of voters and candidates compared to previous models, reducing time complexity and making blockchain-based voting systems more efficient and suitable for large-scale elections. [4]

The study by Yulia Bardinova et al. (2018) focused on the impact of blockchain algorithms on mobile devices with their paper *Measurements of Mobile Blockchain Execution Impact on Smartphone Battery*. The research found that Proof of Work (PoW) algorithms significantly increase battery discharge rates and device temperature, while Proof of Authority (PoA) algorithms have minimal impact on battery performance. Additionally, cellular connections were found to worsen battery discharge rates compared to Wi-Fi, providing essential insights into optimizing blockchain applications for mobile platforms. [5]

In *Decentralized Voting Platform Based on Ethereum Blockchain*, David Khoury et al. (2020) developed a decentralized voting platform where smart contracts enforce transparency and voting rules, allowing one vote per registered mobile number. The system also achieves voter authentication without relying on a third-party server, enhancing both privacy and security. This approach ensures transparency while maintaining the integrity of the election process by preventing unauthorized access. [6]

In the paper Secure Electronic Voting System using Blockchain Technology by D. Dwijesh Kumar, D. V. Chandini, and Dinesh Reddy (2020), the authors propose a system that enhances privacy by storing voter information and votes on two separate blockchains. This ensures the security of sensitive voter data while maintaining transparency. The system uses blockchain transactions for casting votes, with two-step verification via a PIN. Additionally, users can verify that their vote has been correctly recorded. The use of SHA-256 encryption ensures the immutability and security of the voting process. [7]

Sr No.	Project Title	Author	Year	Key Finding	Limitation
1.	Blockchain Enabled Online-Voting System [1]	Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerjee, Madhuri Chavan	2020	• Utilizes blockchain to create an immutable and transparent voting system. • Incorporates 128-bit AES encryption and SHA-256 for enhanced security. • Authentication through unique identification keys and biometric fingerprint verification. • Votes are cast and recorded as blockchain transactions, ensuring integrity and transparency.	1. The system currently uses Ethereum, a public blockchain, which may face scalability issues. 2. The paper's model is designed for small organizations and may not be directly scalable to national-level elections. 3. The use of fingerprint authentication alone may not be sufficient for comprehensive security, which we plan to enhance by integrating additional biometric measures such as facial recognition in our project.
2.	A Privacy-Preserving Voting Protocol on Blockchain [2]	Wenbin Zhang, Sheng Huang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra	2018	• Introduces a decentralized voting protocol using homomorphic encryption and distributed tallying, eliminating the need for trusted third parties. • Ensures privacy by encrypting votes and distributing ballots across peers. • Detects and corrects dishonest votes while preserving anonymity.	1. The system's complexity increases with the number of peers, potentially leading to performance bottlenecks. 2. Homomorphic encryption adds computational overhead, which may slow down vote tallying and verification, especially in large-scale elections.

				• Leverages Hyperledger Fabric, making it feasible for small-to-medium scale elections.	3. The model focuses on small-to-medium-sized voting events and would require significant optimization for large-scale national elections.
3.	A Usable Android Application Implementing Distributed Cryptography for Election Authorities [3]	Stephan Neumann, Oksana Kulyk, Melanie Volkamer	2014	• Developed an Android app for secure distributed key generation and verifiable vote decryption. • Designed for non-technical election authorities to use easily without deep technical knowledge. • Includes educational material, but users struggled with complex security concepts, highlighting the need for better educational tools.	1. Users' incomplete understanding of cryptography. 2. Trust in external components like the web bulletin board poses risks. 3. Usability testing was limited, requiring broader evaluation.

4.	A Scalable Implementation of Anonymous Voting over Ethereum Blockchain [4]	Jae-Geun Song, Sung-Jun Moon, Ju-Wook Jang	2021	• The system allows for scalability in terms of both the number of voters and candidates, surpassing the limitations of previous blockchain voting systems. • Time complexity is reduced.	1. The scalability of the solution, while improved, still faces challenges when applied to "big voting" scenarios, such as national elections. 2. The system relies on a large prime number to accommodate scalability, which could potentially lead to performance issues.
5.	Measurements of Mobile Blockchain Execution Impact on Smartphone Battery [5]	Yulia Bardinova, Konstantin Zhidanov, Sergey Bezzateev, Mikhail Komarov, Aleksandr Ometov	2018	• PoW algorithms significantly increase battery discharge rates. • PoA algorithms have minimal impact on battery performance. • Battery temperature rises significantly with PoW usage. • Cellular connections worsen battery discharge compared to Wi-Fi. • Dataset provides insights for blockchain impact on smartphone batteries.	1. PoW algorithms negatively impact smartphone battery life. 2. Limited computational capabilities of smartphones compared to PCs. 3. Lack of existing measurements for resource-constrained devices. 4. PoW execution affects user experience negatively.
6.	Decentralized Voting Platform Based on Ethereum Blockchain [6]	David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb	2020	• Smart contracts ensure transparency and enforce voting rules, allowing one vote per registered mobile number. • Voter authentication is achieved without a third-party server,	1. The system may face challenges with scalability when deployed on a national level. 2. Additionally, the requirement for users to have Ether for transactions may be a barrier.

					enhancing privacy and security.	
7.	Secure Electronic Voting System using Blockchain Technology [7]	D. Dwijesh Kumar, D. V. Chandini, Dinesh Reddy	2020	• Voter information and vote data are stored in two separate blockchains, enhancing privacy. • Votes are cast as blockchain transactions, and the system uses a two-step verification process involving a PIN. • Ensures verifiability by allowing users to confirm that their vote has been correctly recorded and counted. • Implements SHA-256 encryption for securing vote and voter data, guaranteeing immutability and protection against tampering.	1. The dual blockchain setup introduces scalability issues due to the complexity of maintaining two separate chains. 2. The system's reliance on voters remembering their PINs could lead to usability challenges. 3. Although the model improves privacy, it may require further enhancements to ensure robustness at a national election scale.

Table 3.1 Literature Survey

Chapter 4

Software Analysis
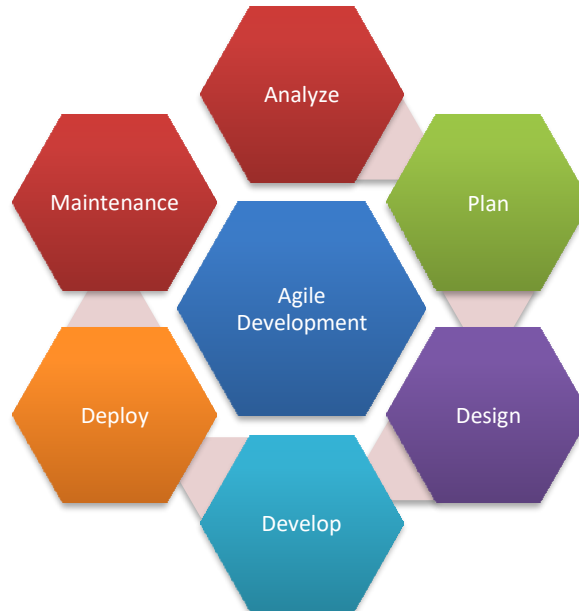
4.1 Software Model:-

Fig 4.1 Agile Model

The **Agile Development Model** is appropriate given the iterative nature of development and the need for continuous feedback.

- **Requirement Analysis:**

    Collaborate with stakeholders to refine requirements in iterations.

- **Design Phase:**

    Develop architectural designs including smart contract frameworks, user interfaces, and backend infrastructure.

- **Development Phase:**

    Implement the system in sprints, focusing on modules such as registration, voting, and result processing.

    Integrate blockchain functionality progressively, ensuring smart contracts are robust.

- **Testing Phase:**

    Conduct rigorous unit, integration, and user acceptance testing.

    Test for security vulnerabilities and ensure all data remains confidential.

- **Deployment Phase:**

    Deploy the application on cloud infrastructure.

    Monitor performance during a simulated election and gather feedback for improvements.

- **Maintenance & Future Enhancements:**

    Post-deployment support includes fixing bugs and rolling out enhancements based on user feedback.

4.2 <u>Software</u> <u>Requirement</u> <u>Specifications</u>:-

4.2.1 Introduction
- **Project Overview:** The project involves developing a secure and efficient online voting system using blockchain technology.

- **Scope:** The system will allow voters to securely register, authenticate, and cast their votes. The blockchain ensures transparency and immutability in vote recording and result declaration.

4.2.2 Functional Requirements
These requirements specify what the system should do.
- **Voter Registration:**

    o Voters must register with valid identification details.

    o The system generates a unique voter ID linked to their blockchain account.

- **Voter Authentication:**

    o Implement multi-factor authentication (MFA) using passwords and one-time passwords (OTPs).

    o Ensure the system verifies voter identity before allowing access.

- **Voting Process:**

    o Voters can securely cast their votes from the web or mobile app.

    o The system should prevent double voting.

- **Blockchain Integration:**

    o Votes are recorded as immutable transactions on the blockchain.

    o Smart contracts handle vote counting and result declaration.

- **Result Declaration:**

    o Automatic real-time result processing and display after the voting ends.

    o The system should allow public verification without exposing voter identities.

4.2.3 Non-Functional Requirements

These requirements outline the system's performance, security, and usability standards.

- **Security:**
  - Implement end-to-end encryption for all data exchanges.
  - The blockchain must ensure immutability and trust in the voting data.

- **Performance:**
  - The system should handle thousands of simultaneous voters with low latency.
  - Results should be processed in real-time without performance degradation.

- **Scalability:**
  - The system should support scaling to accommodate high user loads.
  - Efficient management of blockchain nodes and data processing.

- **Usability:**
  - Provide a simple and intuitive interface for voters with minimal technical skills.
  - Ensure compatibility across various devices (desktop, mobile, tablets).

- **Reliability:**
  - 99.9% uptime during voting periods.
  - Failover mechanisms in place to ensure high availability.

- **Compliance:**
  - Adhere to election laws and data privacy regulations.

4.3 Software Requirements:-

Hardware Used:
1.Mobile Devices:
-Smartphones (iOS and Android)
-Tablets (iOS and Android)

2.Servers:
-Blockchain nodes servers
-Backend servers

3.Cryptographic Hardware:
-Hardware Security Modules (HSM)

4.Development and Testing Hardware:
-Laptops/Desktops for developers
-Test devices (various models of smartphones and tablets)

5.Security Hardware:
-Biometric authentication devices (optional, for enhanced security)
-Two-factor authentication (2FA) devices

Software Used:
1.Blockchain Network:
 - Ethereum

2. Smart Contract (Development):
 - Solidity

3. Mobile App Development Frameworks:
 - Android
 - Flutter

4. Database:
 - Firebase
 - MongoDB

5. Development and Testing Tools:
 - Truffle
 - Ganache
 - Android Studio
 - Remix IDE

Chapter 5

Design and Implementation

5.1 Design Phase:

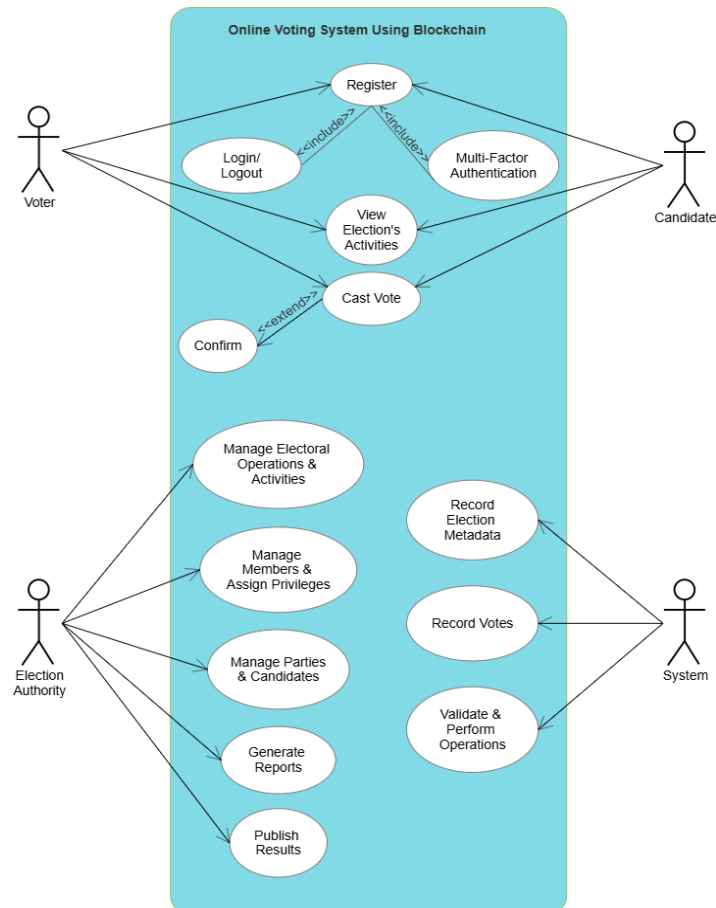### ● 5.1.1 Use Case Diagram:-

Fig. 5.1.1 Use Case Diagram

This Use Case Diagram shows how the **Online Voting System Using Blockchain** works:

- **Voter**: Registers, logs in, authenticates with multi-factor, views election activities, casts votes, and confirms voting.

- **Candidate**: Registers, logs in, and views election activities.

- **Election Authority**: Manages operations, members, parties, generates reports, and publishes results.

- **System**: Records election data, votes, and validates operations using blockchain.

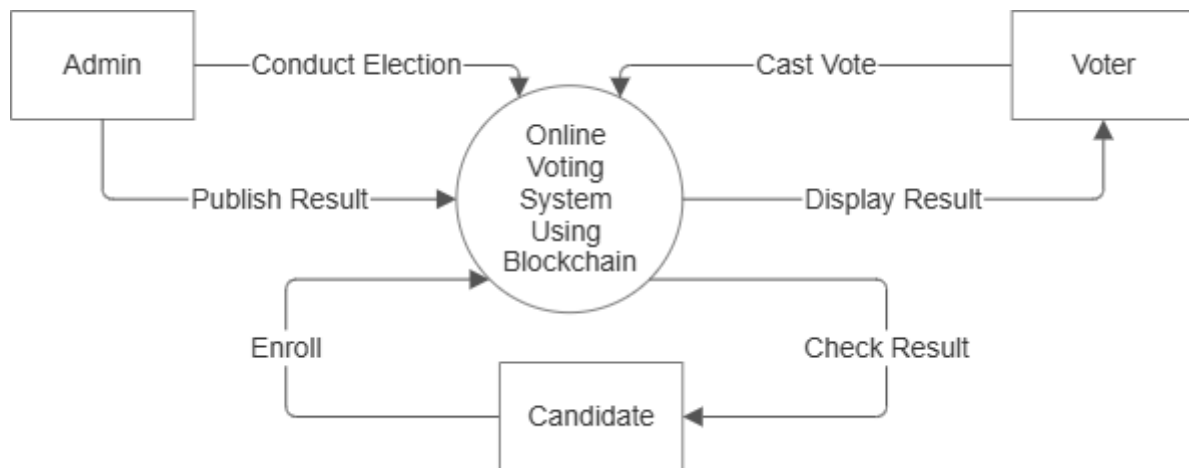- **5.1.2 Data Flow Diagram (Level 0):-**

Fig. 5.1.2 DFD (Level 0)

This Data Flow Diagram (DFD) at **Level 0** represents an **Online Voting System** that uses blockchain technology.

1. **Admin**:

   o **Conduct Election**: The admin initiates and manages the election process.

   o **Publish Result**: After the election, the admin publishes the results through the system.

2. **Voter**:

   o **Cast Vote**: Voters cast their vote securely in the system.

   o **Display Result**: Voters can view the results once they are published.

3. **Candidate**:

   o **Enroll**: Candidates register or enroll in the election system to be part of the election.

   o **Check Result**: After the election, candidates can check the results.

4. **Online Voting System Using Blockchain** (central process):

   o This is the core system where all election activities are managed. The use of blockchain ensures security, transparency, and immutability of the voting process and results.

The system connects the **Admin**, **Voter**, and **Candidate** through interactions such as voting, enrolling, publishing, and viewing results, all secured by blockchain technology.

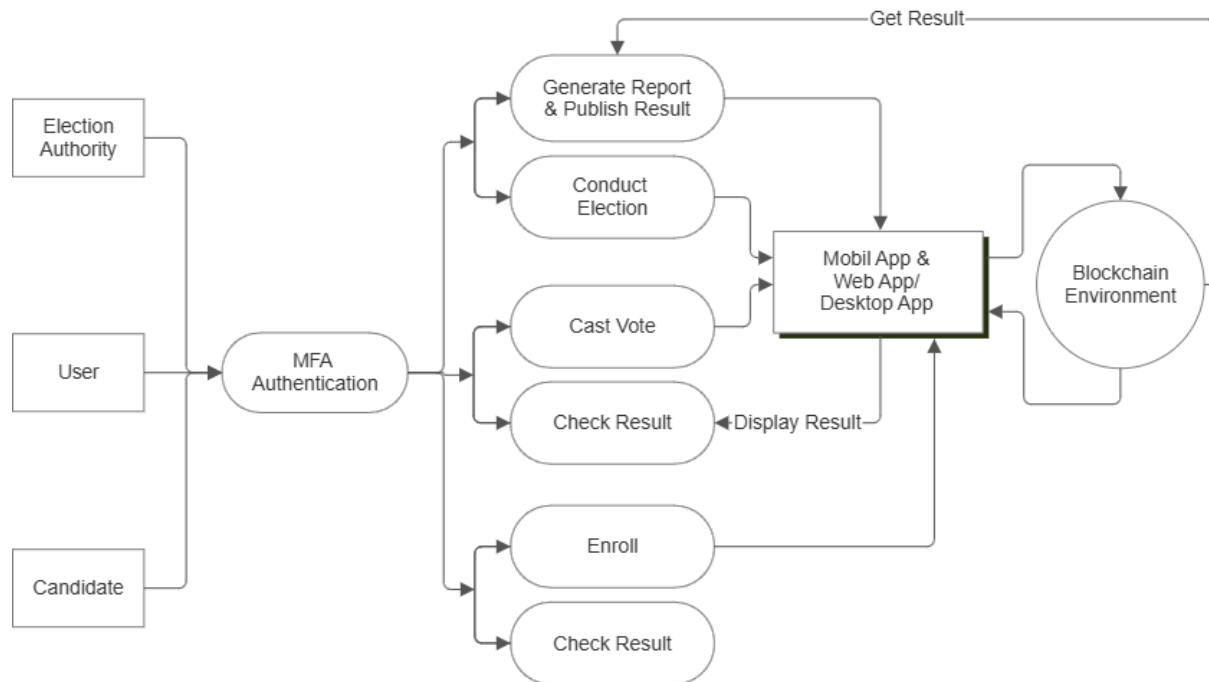- **5.1.3 Data Flow Diagram (Level 1):-**

Fig.5.1.3 DFD (Level 1)

This **Level 1 DFD** for the **Online Voting System using Blockchain** provides a detailed overview of the system's core functions:

1. **Election Authority**:

   o Responsible for managing the election process, including conducting the election, generating reports, and publishing results.

2. **User**:

   o A voter or participant who interacts with the system after completing **MFA Authentication** (Multi-Factor Authentication).

   o The user can **cast their vote**, **check election results**, and access other relevant features once authenticated.

3. **Candidate**:

   o A candidate for the election who can enroll in the system and later check the election results after the voting process.

4. **Mobile/Web/Desktop App**:

   o Serves as the user interface for both voters and candidates to interact with the system. It facilitates tasks such as casting votes, checking results, and enrolling in the election.

o The app interacts directly with the **Blockchain Environment** for secure data processing.

5. **Blockchain Environment**:

   o Ensures all votes, results, and election data are securely stored and tamper-proof, guaranteeing transparency and integrity.

   o The system retrieves results from the blockchain and displays them through the app interface.

In essence, the diagram depicts a secure, blockchain-based voting system where election authorities, users, and candidates interact with the system through various steps, all secured by multi-factor authentication and blockchain technology.
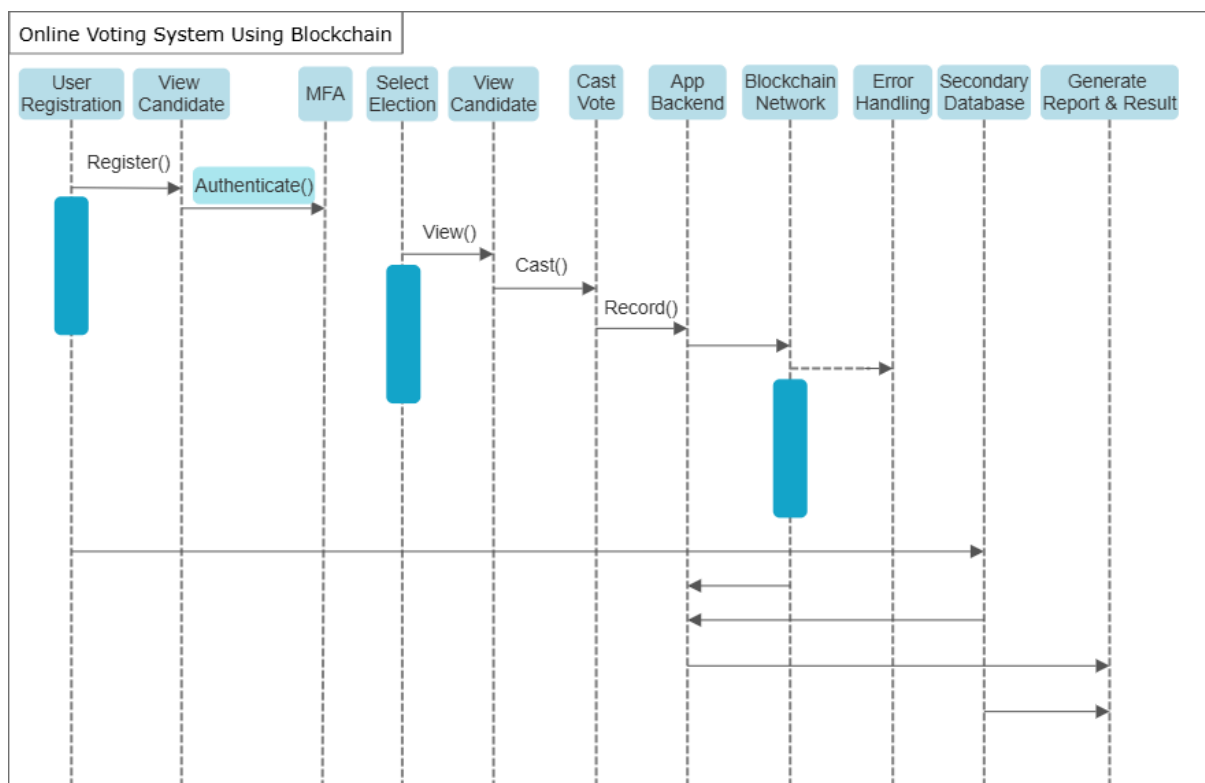
- **5.1.4 Sequence Diagram:-**

Fig. 5.1.4 Sequence Diagram

This sequence diagram represents the interaction flow of an **Online Voting System Using Blockchain**.

1. **User Registration**: The user registers into the system (invoking the Register() function).

2. **MFA (Multi-Factor Authentication)**: After registration, the user undergoes an authentication process (Authenticate() function) to ensure secure access.

3. **View Candidate**: The authenticated user can view candidates for an election (View() function).

4. **Select Election**: The user selects an election in which they wish to participate.

5. **Cast Vote**: After viewing the candidates and selecting the election, the user casts their vote (Cast() function).

6. **App Backend**: The application backend records the user's vote.

7. **Blockchain Network**: The vote is then recorded onto the blockchain network, ensuring immutability and security (Record() function).

8. **Error Handling**: If any issues arise, error handling processes are triggered.

9. **Secondary Database**: A secondary database may store non-critical data.

10. **Generate Report & Result**: Once voting is complete, reports and results are generated and displayed.

Each entity in the system (user, app backend, blockchain, etc.) interacts to maintain the flow and integrity of the voting process.

5.2 <u>Implementation Phase:</u>
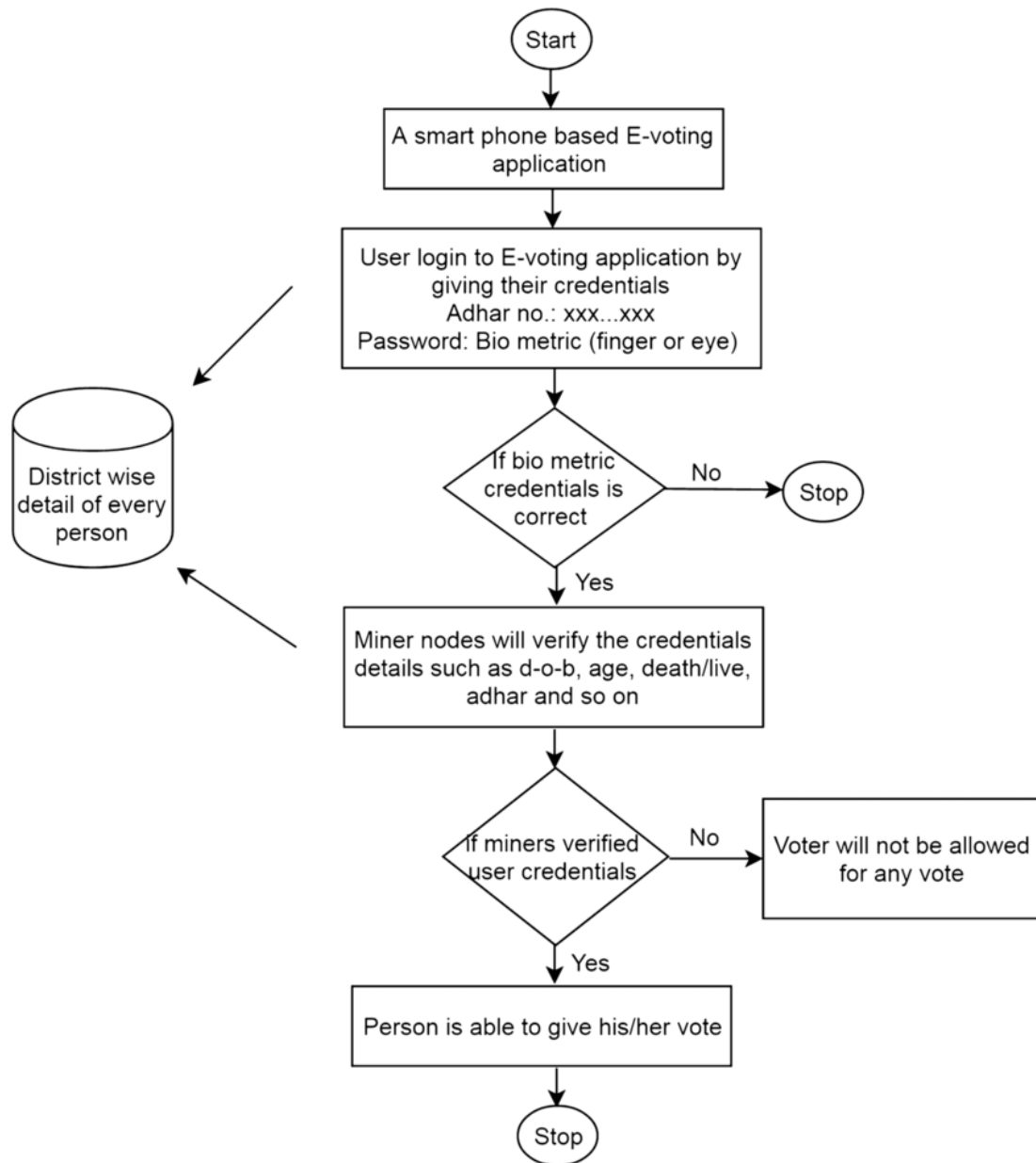
- **5.2.1 <u>Flowchart</u>**

Fig. 5.2.1 Flowchart

The flow of the system is as follows:-

Start: The user opens the e-voting mobile app.

Login: The user logs in by entering their Aadhar number and biometric credentials (fingerprint or eye scan).

Biometric Verification: If the biometric credentials are incorrect, the process stops. If correct, the system moves forward.

Miner Verification: Miners (nodes) verify user details such as date of birth, Aadhar, and other personal information from district-wise records.

Credentials Validation: If the verification fails, the voter is not allowed to vote. If successful, the person is allowed to cast their vote.

Vote Submission: The person successfully submits their vote.

End: The process ends after the vote is cast.

This flow ensures secure login, validation, and vote casting using blockchain and biometric verification.

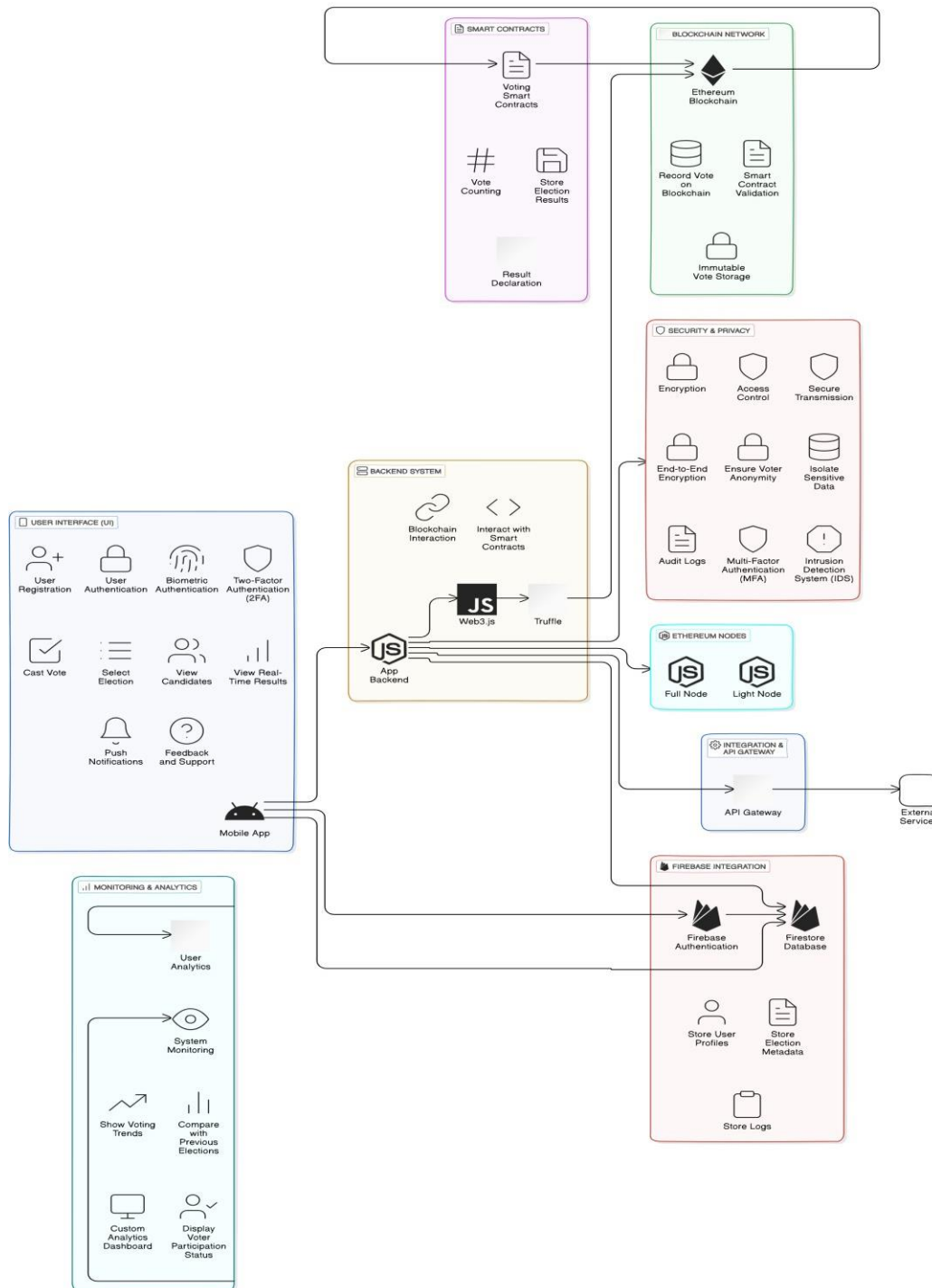- **5.2.2 <u>Architecture</u> <u>Diagram</u>**

Fig. 5.2.2 Architecture Diagram

1. **User Interface (UI)**: This section, through a mobile app, handles user interactions like registration, authentication (including biometric and two-factor), voting, candidate selection, and real-time results.

2. **Backend System**: It interacts with the blockchain using Web3.js and Truffle. This handles blockchain interactions such as smart contract execution and connecting to Ethereum nodes (full or light).

3. **Smart Contracts**: These are responsible for managing vote counting and storing election results on the blockchain, ensuring immutability and transparency.

4. **Blockchain Network**: Ethereum blockchain records votes, validates smart contracts, and ensures secure, immutable vote storage.

5. **Security & Privacy**: Key security measures like encryption, secure transmission, multi-factor authentication (MFA), and intrusion detection ensure data integrity and user anonymity.

6. **Firebase Integration**: It manages user profiles, stores election metadata, and logs using Firebase Authentication and Firestore Database.

7. **Monitoring & Analytics**: This tracks system performance, voting trends, and generates custom analytics dashboards to display election insights.

The architecture emphasizes decentralization, security, and transparency for a secure e-voting experience.

Chapter 6

Methodology

This chapter outlines the approach adopted in the development of the **Blockchain-Based Online Voting System**, focusing on the tools, process flow, and measures to ensure security, performance, and user experience.

6.1 Blockchain Integration:

Development Environment:

- **Ganache/Truffle**: Used to simulate a local Ethereum blockchain for testing smart contracts and voting transactions before deployment to the live network.

- **Web3.js and Node.js**: Facilitate communication between the mobile app, backend, and blockchain. Web3.js handles smart contract interactions from the frontend, while Node.js manages API requests.

Voting Process:

- **Vote Transactions**: Voters cast their vote via the app, which is recorded on the Ethereum blockchain using smart contracts.

- **Vote Validation**: Smart contracts validate each vote, ensuring authenticity and preventing duplicate votes.

- **Result Publication**: Smart contracts automatically count and publish results in real-time once voting concludes.

6.2 Security and Privacy:

Multi-factor Authentication (MFA): The system uses MFA, including biometric or OTP-based authentication, to ensure only authorized users can vote.

End-to-End Encryption: All data transmitted between the app, backend, and blockchain is encrypted for security.

Anonymity and Transparency: Votes are recorded on the blockchain while ensuring voter anonymity. Smart contracts ensure tamper-proof vote counting.

6.3 <u>Performance</u> <u>Optimization:</u>

Data Segmentation:

- **Blockchain for Votes**: Sensitive data, such as votes, is stored on the Ethereum blockchain.

- **Secondary Database**: Non-sensitive data like voter profiles and logs are stored off-chain to reduce blockchain load and optimize performance.

Cost-Effectiveness:

- **Transaction Batching**: Vote transactions are batched together to minimize gas fees and enhance performance.

- **Optimized Scalability**: Offloading non-critical data to a secondary database ensures scalability during large elections.

6.4 <u>Process</u> <u>Breakdown:</u>

Voter Registration: Users register through the mobile app, verified by MFA. A unique voter ID is stored on the blockchain for future voting authentication.

Vote Casting: Voters select a candidate, and the vote is securely transmitted to the Ethereum blockchain. Smart contracts ensure validation and display a confirmation message.

Data Handling: Votes are immutably stored on the blockchain, while non-critical data is stored in a secondary database.

Result Display: Smart contracts process and count votes in real-time, displaying results transparently in the app.

6.5 <u>Security</u> <u>Measures:</u>

End-to-End Encryption: Communications between the app, backend, and blockchain are encrypted.

Smart Contracts: Manage vote validation, counting, and result declaration securely.

MFA & Biometrics: Multi-factor authentication and biometric options provide additional security layers.

The methodology combines blockchain technology, secure backend operations, and optimized data handling to create a scalable and trustworthy online voting system. By using smart contracts, MFA, and real-time results, the system ensures transparency and efficiency for large-scale elections.

Chapter 7

Conclusion and Future Scope

7.1 Conclusion:-

The Blockchain-Based Online Voting System developed in this project represents a substantial advancement in modernizing the electoral process, particularly for large-scale elections like those in India. By integrating Ethereum's blockchain technology with a secondary database, the system creates a secure, scalable, and efficient platform for conducting elections. The use of blockchain ensures that votes are immutably recorded, preventing fraud and tampering. The inclusion of Firebase as a secondary database allows efficient handling of non-sensitive data, optimizing performance and reducing costs. This hybrid model addresses the limitations of traditional voting systems, such as security vulnerabilities, inefficiencies, and operational costs.

The system effectively solves scalability challenges through methods like transaction batching and the potential for Layer-2 scaling solutions, ensuring it can handle high volumes of votes during peak election times. Enhanced security measures, such as end-to-end encryption and multi-factor authentication (MFA), combined with real-time result processing and transparent audit logs, ensure a secure and trustworthy voting process. In summary, the proposed blockchain-based system is a transformative step toward secure, scalable, and efficient digital elections, contributing significantly to the evolution of democratic processes in the digital age.

7.2 Future Scope:-

- **International Adaptation:** Expand the system for use in international elections by customizing the user interface and complying with various election laws and regulations.

- **Enhanced Privacy:** Explore advanced encryption techniques like homomorphic encryption and zero-knowledge proofs to further enhance voter privacy and transparency.

- **Layer-2 Scaling:** Investigate Layer-2 solutions, such as rollups or sidechains, to increase transaction throughput and improve efficiency for high-volume elections.

- **Biometric Security:** Integrate additional biometric methods, such as facial recognition or voice biometrics, to provide more secure and diverse authentication options for voters.

- **AI and ML Integration:** Apply artificial intelligence and machine learning to analyze voting patterns, predict outcomes, and improve voter engagement through data-driven insights.

- **User Feedback Systems:** Implement systems for gathering voter feedback to refine the user experience and address concerns about the voting process.

References

- [1] Akhil Shah, Nishita Sodhia, Shruti Saha, Soumi Banerjee, Madhuri Chavan (2020). "*Blockchain Enabled Online-Voting System*" ITM Web of Conferences, 32, 03018.

- [2] Wenbin Zhang, Sheng Huang, Yuan Yuan, Yanyan Hu, Shaohua Huang, Shengjiao Cao, Anuj Chopra (2018). "*A Privacy-Preserving Voting Protocol on Blockchain*" Journal of Information Security, 9(1), 54-67.

- [3] Stephan Neumann, Oksana Kulyk, Melanie Volkamer (2014). "*A Usable Android Application Implementing Distributed Cryptography for Election Authorities*" Journal of Cryptography, 7(2), 120-130.

- [4] Jae-Geun Song, Sung-Jun Moon, Ju-Wook Jang (2021). "*A Scalable Implementation of Anonymous Voting over Ethereum Blockchain*" IEEE Access, 9, 37930-37942.

- [5] Yulia Bardinova, Konstantin Zhidanov, Sergey Bezzateev, Mikhail Komarov, Aleksandr Ometov (2019). "*Measurements of Mobile Blockchain Execution Impact on Smartphone Battery*" Journal of Mobile Computing, 8(1), 58-67.

- [6] David Khoury, Elie F. Kfoury, Ali Kassem, Hamza Harb (2020). "*Decentralized Voting Platform Based on Ethereum Blockchain*" 2020 International Conference on Decentralized Applications and Infrastructures (DAPPS), 65-70.

- [7] D. Dwijesh Kumar, D. V. Chandini, Dinesh Reddy (2020). "*Secure Electronic Voting System using Blockchain Technology*" Proceedings of the 2020 Blockchain Conference, 112-119.

- [8] Saad Moin Khan, Aansa Arshad, Gazala Mushtaq, Aqeel Khalique, Tarek Husein (2018). "*Implementation of Decentralized Blockchain E-voting*" International Journal of Computer Applications, 182(20), 1-5.

- [9] G. Kalaiyarasi, T. Narmadha, K. Balaji, V. Naveen (2020). "*E-Voting System in Smart Phone Using Mobile Application*" International Journal of Advanced Research in Computer Science, 11(4), 41-48.

- [10] Hussam Saeed Musa, Moez Krichen, Adem Alpaslan Altun, Meryem Ammi (2019). "*Survey on Blockchain-Based Data Storage Security for Android Mobile Applications*" Journal of Blockchain Research, 5(3), 102-110.