CHAPTER 1

INTRODUCTION

Blockchain technology has emerged as a transformative force with the potential to revolutionize various facets of our society, and one area where its impact could be particularly profound is in the electoral process. By leveraging blockchain for digital elections, numerous benefits can be realized, ranging from enhanced security and transparency to significant cost savings and improved voter trust.

At its core, [1]. blockchain technology offers a decentralized and immutable ledger system, where transactions are recorded across a network of computers in a transparent and secure manner. This inherent design makes it an ideal candidate for ensuring the integrity of the voting process. Unlike traditional digital voting systems that rely on centralized databases, which are vulnerable to hacking and manipulation, blockchain decentralizes data storage, making it extremely difficult for any single entity to compromise the integrity of the system.

One of the key advantages of [6]. blockchain-based voting systems is their resilience to tampering and fraud. Each vote cast is recorded as a transaction on the blockchain, and once added to the ledger, it cannot be altered or deleted. This not only ensures the accuracy and integrity of the electoral results but also provides voters with confidence that their voices are being accurately represented.

Furthermore, [11]. blockchain technology can streamline various aspects of the electoral process, leading to cost savings and improved efficiency. By eliminating the need for physical polling stations and voting machines, resources can be reallocated to support blockchain miners who verify and validate transactions on the network. This not only reduces operational costs but also minimizes the logistical challenges associated with traditional voting methods, such as staffing and security.

Moreover, [4]. blockchain-based voting systems offer enhanced transparency, as all transactions are recorded on a public ledger that is accessible to anyone. This transparency not only allows voters to verify that their votes have been accurately counted but also enables independent audits to ensure the integrity of the electoral process. Additionally, blockchain technology can facilitate secure and verifiable remote voting, enabling greater accessibility and participation in the democratic process.

Beyond the electoral process, blockchain technology has demonstrated its value in a wide range of industries, including banking, healthcare, and food safety. Its ability to provide secure, transparent, and tamper-proof record-keeping makes it an ideal solution for any application that requires trust and accountability.

In conclusion, blockchain technology holds tremendous promise for transforming the electoral process. By leveraging its inherent security, transparency, and efficiency, blockchain-based voting systems have the potential to enhance trust, integrity, and participation in democratic elections. However, it is essential to address any potential challenges and ensure that appropriate safeguards are in place to protect the integrity of the voting process and safeguard voter confidentiality. With careful implementation and ongoing innovation, blockchain technology could revolutionize the way we conduct elections and uphold the principles of democracy in the digital age.

1.1 Motivation

Developing a blockchain-based voting system integrated with face recognition and one-time passwords (OTPs) stems from a confluence of motivations, driven primarily by the need for enhanced security, transparency, and accessibility in electoral processes.

First and foremost, security is paramount in any voting system. By utilizing blockchain technology, which offers immutable and transparent record-keeping, the Authenticity of the voting process can be significantly bolstered. Each vote cast is cryptographically secured and Archived on a Distributed ledger, making it practically impossible for malicious actors to tamper with or manipulate the results without detection. The addition of face recognition technology adds an extra layer of authentication, guaranteeing that only Qualified voters are Capable to participate, thereby mitigating the risks associated with identity fraud and impersonation. Moreover, the incorporation of OTPs further fortifies the security of the voting system by providing a unique and time-sensitive code to each voter, which must be inputted alongside their facial recognition scan before their vote is registered. This two-factor authentication mechanism helps safeguard against unauthorized access and ensures that only legitimate voters are able to cast their ballots, thereby reducing the likelihood of fraudulent activities such as ballot stuffing or coercion.

Beyond security concerns, blockchain-based voting systems offer unparalleled transparency and auditability, enabling voters to independently verify that their votes have been accurately recorded and counted. By leveraging blockchain's decentralized nature, the entire voting process becomes transparent and auditable in real-time, fostering trust and confidence in the electoral outcome. This transparency not only enhances the legitimacy of the electoral process but also serves as a deterrent against attempts to undermine the integrity of the vote.

Furthermore, the adoption of Epic voter id, face recognition technology and OTPs enhance the accessibility of the voting process, particularly for individuals with disabilities or those who may face logistical challenges in accessing traditional polling stations. By enabling voters to cast their ballots remotely using a secure digital platform, blockchain-based voting systems can help increase voter turnout and promote inclusivity in the democratic process.

CHAPTER 2

LITERATURE SURVEY

[1]. **Title of Paper :**The application of blockchain technology in voting systems: A review. ACM Computer Survey, 54(3), 1–28.

Authors: Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K.-K.-R. (2022).

This paper presents a comprehensive review of the application of blockchain technology in voting systems. It discusses various aspects such as security, transparency, scalability, and privacy concerns related to blockchain-based voting systems. The authors explore different blockchain-based voting architectures, consensus mechanisms, and implementation challenges. Additionally, the paper examines case studies and real-world deployments of blockchain in voting systems to highlight both the opportunities and challenges associated with this technology.

Remark:

This review provides valuable insights into the potential of blockchain technology to enhance the security and transparency of voting systems. It serves as a useful resource for researchers, policymakers, and practitioners interested in understanding the implications of adopting blockchain in the context of elections.

[2]. **Title of Paper :**Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers-Plymouth University. Accessed: Feb. 14.

Authors: Barnes, C., Brake, C., & Perry, T. (2022).

This document likely presents a research or project report from the Plymouth University's Team Plymouth Pioneers, focusing on digital voting utilizing blockchain technology. It might detail the design, development, and testing of a blockchain-based voting system by the team. The report could discuss the technical architecture, implementation challenges, and outcomes of their digital voting solution

Remark: While specific details about the content and findings of the report are not provided, it represents a practical application of blockchain in the context of voting systems, contributing to the growing body of research and experimentation in this field.

[3]. **Title of Paper:** Going from bad to worse: From internet voting to blockchain voting.

Authors : J. Cybersecurity, 7(1), 1–15.

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021).

This journal article critically evaluates the transition from internet voting to blockchain-based voting systems. It examines the potential risks and vulnerabilities associated with blockchain voting, contrasting them with the shortcomings of internet voting. The authors highlight security concerns, including the threat of cyberattacks, manipulation, and coercion in blockchain-based voting systems.

Remark:

This article offers a cautionary perspective on the adoption of blockchain in voting systems, emphasizing the need for rigorous security measures and careful consideration of the potential pitfalls associated with this technology.

[4]. **Title of Paper :**On the design and implementation of a blockchain-enabled E-Voting application within IoT-oriented smart cities. IEEE Access, 9, 34165–34176.

Authors: Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021**).** This paper presents a study on the design and implementation of a blockchain-enabled electronic voting (E-Voting) application tailored for IoT-oriented smart cities. It likely discusses the integration of blockchain technology with IoT devices to create a secure and transparent voting system. The authors might detail the architecture, features, and challenges encountered in developing and deploying the E-Voting application.

Remark:

The focus on integrating blockchain with IoT devices for E-Voting in smart cities highlights the potential synergy between emerging technologies to address challenges in democratic processes. This research contributes to the exploration of innovative solutions for enhancing voting systems in urban environments.

[5]. **Title of Paper :**Efficient, coercion-free and universally verifiable blockchain-based voting. Computer Network, 174, Art. no. 107234.

Authors: Dimitriou, T. (2020).

This article proposes an efficient and coercion-free blockchain-based voting system that ensures universal verifiability. It likely introduces novel cryptographic techniques or consensus mechanisms to address challenges such as vote manipulation and coercion in traditional voting systems. The author might provide a theoretical framework and possibly a proof-of-concept implementation to demonstrate the feasibility and effectiveness of the proposed voting system.

Remark:

The emphasis on coercion-free and universally verifiable voting aligns with the core principles of democratic elections. This research contributes to the ongoing efforts to design secure and transparent voting systems using blockchain technology.

[6]. **Title of Paper:** A framework to make charity collection transparent and auditable using blockchain technology. Comput. Electr. Eng., 83, Art. no. 106588.

Authors: Farooq, M. S., Khan, M., & Abid, A. (2020).

This paper presents a framework for leveraging blockchain technology to enhance transparency and auditability in charity collection processes. It likely discusses the design and implementation of a blockchain-based platform for tracking donations, ensuring that funds are used as intended, and providing stakeholders with verifiable proof of transactions. The authors might also examine the potential impact of blockchain on improving trust and accountability in charitable activities.

Remark:

While not directly related to voting systems, this research showcases the versatility of blockchain technology in promoting transparency and accountability in various domains. The principles and techniques proposed could potentially be adapted for use in voting systems to enhance trust and integrity.

[7]. **Title of Paper**: An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron.

Authors: Kim, T., Ochoa, J., Faika, T., Mantooth, A., Di, J., Li, Q., & Lee, Y. (2020**).**

This article provides an overview of the cyber-physical security challenges associated with battery management systems (BMS) and explores the adoption of blockchain technology to address these challenges. While the focus is primarily on BMS, the paper might discuss how similar security principles could be applied to other cyber-physical systems, including voting systems, to enhance security, reliability, and trust.

Remark:

Although not directly related to voting systems, this overview underscores the importance of addressing cybersecurity concerns in critical systems. The discussion on leveraging blockchain technology for enhancing security could inspire further research into its application in securing voting systems against cyber threats.

[8]. **Title of Paper:** This paper offers an overview of the potential impact of blockchain technology on financial services.

Authors: Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020).

It likely discusses the various ways blockchain is transforming traditional financial processes, such as payments, clearing, and settlement. The authors might also highlight the challenges and barriers to widespread blockchain adoption in the financial sector, along with recommendations for addressing them based on insights from expert interviews

Remark:

While the primary focus is on financial services, the insights and recommendations provided could have implications for other sectors, including voting systems. Understanding the challenges and strategies for overcoming them in the financial domain may inform similar efforts to integrate blockchain into voting processes securely and effectively.

[9]. **Title of Paper**: An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access, 8, 103994–104015.

Authors: Ometov, A., Bardinova, Y., Afanasyeva, A., Masek, P., Zhidanov, K., Vanurin, S., Sayfullin, M., Shubina, V., Komarov, M., & Bezzateev, S. (2020).

This overview provides insights into the state-of-the-art developments in blockchain technology for smartphones. It likely covers topics such as blockchain-based applications, consensus mechanisms suitable for resource-constrained devices, implementation challenges, and future trends. The authors might discuss the potential use cases of blockchain on smartphones and its implications for various industries, including governance and voting.

Remark:

Although the focus is on smartphones, the discussion on implementing blockchain in resource-constrained environments may offer valuable insights for designing efficient and accessible voting systems. Exploring blockchain's potential to empower voters through mobile devices could inform the development of inclusive and user-friendly voting solutions.

[10]. **Title of Paper:** Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Netw., 34, 8–14.

Authors: Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020).

This article explores the role of blockchain technology in enhancing the security of smart cities. It likely discusses the architecture, requirements, and challenges associated with deploying blockchain solutions in urban environments to secure critical infrastructure and services. The authors might propose strategies for leveraging blockchain to mitigate cybersecurity risks and ensure the integrity of data and transactions in smart city applications, which could include voting systems.

Remark:

While the primary focus is on smart city infrastructure, the discussion on securing critical services through blockchain technology could have implications for voting systems in urban settings. Understanding the architecture and requirements for deploying blockchain in smart cities may inform the development of secure and resilient voting platforms for urban populations.

[11].**Title Of Paper:** A survey on the feasibility and suitability of blockchain techniques for e-voting systems. arXiv, arXiv:2002.07175.

Authors: Cabuk, U. C., Adiguzel, E., & Karaarslan, E. (2020).

This survey paper explores the feasibility and suitability of employing blockchain techniques in electronic voting (e-voting) systems. It likely assesses the potential benefits and challenges of integrating blockchain technology into existing e-voting infrastructure. The authors might analyze different blockchain architectures, consensus mechanisms, and security considerations relevant to e-voting, providing insights into the practicality and effectiveness of blockchain-based solutions.

Remark:

This survey contributes to the understanding of the applicability of blockchain in e-voting systems, offering valuable insights into the technical and operational considerations that need to be addressed for successful implementation. By evaluating the feasibility and suitability of blockchain techniques, this research informs decision-making processes regarding the adoption of blockchain in electoral processes.

[12].**Title of Paper:** A novel service level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0. Enterp. Inf.Syst.

Authors: Zhu, W., Tan, H., Zhao, J., Da Xu, L., & Guo, K. (2021).

This paper presents a novel service level agreement (SLA) model that leverages blockchain and smart contracts to facilitate cloud manufacturing in the context of Industry 4.0. It likely discusses how blockchain technology can enhance transparency, trust, and automation in SLA management for cloud-based manufacturing services. The authors might propose a framework or prototype implementation demonstrating the integration of blockchain and smart contracts to enforce SLAs effectively.

Remark:

While the primary focus is on cloud manufacturing, the utilization of blockchain and smart contracts to enforce agreements and ensure accountability has broader implications. This research highlights the potential for blockchain technology to streamline contractual processes and enhance trust in various domains, including voting systems.

[13].**Title of Paper:** A Study on Public Blockchain Consensus Algorithms: A Systematic Literature Review. Preprints.

Authors: Shukur, I., Bakar, Z., & Bakar, K. A. A. (2020).

This study conducts a systematic literature review on public blockchain consensus algorithms. It likely examines different consensus mechanisms used in public blockchains, such as Proof of Work (PoW), Proof of Stake (PoS), and variations thereof. The authors might analyze the characteristics, advantages, and limitations of each consensus algorithm, providing insights into their suitability for various blockchain applications, including voting systems.

Remark:

While not directly focused on voting systems, this systematic literature review offers valuable insights into the consensus mechanisms that underpin blockchain technology. Understanding the properties and performance of consensus algorithms is crucial for designing secure and efficient blockchain-based voting systems.

[14].**Title Of Paper: Blockchain and Cryptocurrencies. J. Risk Financ. Manag., 13, 227**.

Authors: Chan, S., Chu, J., Zhang, Y., & Nadarajah, S. (2020**).**

This article explores the intersection of blockchain technology and cryptocurrencies. It likely discusses the fundamental concepts of blockchain, its applications beyond cryptocurrencies, and the implications for finance and risk management. The authors might analyze the potential benefits and challenges of integrating blockchain into financial processes and discuss regulatory considerations.

Remark:

While primarily focused on finance, this article provides insights into the broader implications of blockchain technology. Understanding the relationship between blockchain and cryptocurrencies may inform discussions on leveraging blockchain for secure and transparent financial transactions, including those related to voting systems.

[15]. **Title of Paper: E-voting scan integrity: End-to-end voter verifiable optical-scan voting**. IEEE Security. Privacy, 6(3), 40–46.

Authors: Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., & Vora, P. (2008**).**

This article discusses end-to-end verifiable voting systems, specifically focusing on optical-scan voting with an emphasis on maintaining the integrity of the voting process. It likely presents a detailed examination of the technical aspects of optical-scan voting, including cryptographic protocols and verification mechanisms. The authors may also discuss practical considerations and challenges associated with implementing such systems in real-world elections.

Remark:

This paper predates the recent surge in blockchain technology's application in voting systems but provides insights into alternative approaches for ensuring the integrity and verifiability of voting processes. While not directly related to blockchain, the principles discussed align with the goals of transparency and trustworthiness sought in blockchain-based voting systems.

2.1 Detailed review and comparison of literature survey.

REF. No	Title	Description	Limitation	Motivation
1.	The application of blockchain technology in voting systems: A review.	This paper reviews the application of blockchain technology in voting systems, focusing on security, transparency, scalability, and privacy concerns. It examines various	Lacks detailed analysis of scalability solutions and long-term sustainability.	Enhance security and transparency in voting systems.

		blockchain voting architectures, consensus mechanisms, implementation challenges, and real-world deployments.		
2.	Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers-Plymouth University.	This document likely details the design, development, and testing of a blockchain-based voting system by Plymouth University's Team Plymouth Pioneers, discussing technical architecture and implementation outcomes.	The specific details about the report's findings and methodologies are not provided, potentially limiting the depth of insights.	To demonstrate a practical application of blockchain in voting systems, contributing to the body of research through real-world experimentation and implementation.
3.	Going from bad to worse: From internet voting to blockchain voting.	This article critically evaluates the transition from internet voting to blockchain-based voting, highlighting potential risks and vulnerabilities, and contrasting them with those of	It focuses primarily on the risks and may not sufficiently explore potential solutions or the positive aspects of blockchain voting systems.	To provide a cautionary perspective on blockchain voting, emphasizing the need for rigorous security measures and

		internet voting.		careful consideration of potential pitfalls.
4.	On the design and implementation of a blockchain-enabled E-Voting application within IoT oriented smart cities	The study discusses the design and implementation of a blockchain-enabled electronic voting application for IoT-oriented smart cities, integrating blockchain with IoT devices for secure voting.	The paper might face challenges in addressing the scalability and interoperability of blockchain with various IoT devices.	To explore innovative solutions for enhancing voting systems in urban environments by leveraging the synergy between blockchain and IoT technologies.
5.	Efficient, coercion-free and universally verifiable blockchain-based voting	This article proposes a blockchain-based voting system that is efficient, coercion-free, and universally verifiable, introducing cryptographic techniques to prevent vote manipulation.	The theoretical framework might lack comprehensive real-world testing or proof-of-concept implementations.	To design a secure and transparent voting system that aligns with the core principles of democratic elections, focusing on preventing coercion and ensuring verifiability.

6.	A framework to make charity collection transparent and auditable using blockchain technology	The paper presents a framework for enhancing transparency and auditability in charity collection processes using blockchain technology.	While focused on charity collection, the principles may need adaptation for direct application in voting systems.	To showcase blockchain's potential in promoting transparency and accountability, principles which could be adapted to improve voting systems.
7.	An overview of cyber-physical security of battery management systems and adoption of blockchain technology	This article discusses cyber-physical security challenges in battery management systems and explores the adoption of blockchain to enhance security.	The primary focus is on battery management systems, making direct applicability to voting systems less immediate.	To address cybersecurity concerns in critical systems, providing insights that could inspire research into securing voting systems using blockchain.
8.	How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees.	The paper explores the impact of blockchain on financial services, discussing transformations in payments, clearing, and settlement processes.	The focus on financial services might limit direct relevance to voting systems without adaptation of the discussed principles.	To understand blockchain's transformative potential in finance, with implications for secure and transparent transactions that

				can inform voting system enhancements.
9.	An Overview on Blockchain for Smartphones: State-of-the-Art,Consensus, Implementation, Challenges and Future Trends	This overview discusses the state-of-the-art in blockchain for smartphones, covering applications, consensus mechanisms, implementation challenges, and future trends.	The emphasis on smartphones may require additional considerations for implementing blockchain in voting systems.	To explore blockchain applications in resource-constrained environments, providing insights for developing efficient and accessible voting solutions.
10.	Securing smart cities through blockchain technology: Architecture, requirements, and challenges.	This article examines the role of blockchain in enhancing smart city security, discussing architecture, requirements, and deployment challenges.	The broad focus on smart cities might dilute specific insights related to voting systems.	To secure critical urban services through blockchain, with strategies that could be adapted to enhance voting system security in smart cities.
11.	A survey on the feasibility and suitability of blockchain techniques for e-	This survey assesses the feasibility and suitability of blockchain in	The survey might not provide detailed case studies or real-world	To evaluate blockchain's practicality and effectiveness in e-voting,

	voting systems.	electronic voting systems, analyzing different architectures, consensus mechanisms, and security considerations.	implementation results.	informing decision-making for adopting blockchain in electoral processes.
12.	A novel service level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0	his paper proposes an SLA model using blockchain and smart contracts for cloud manufacturing, enhancing transparency and automation in SLA management.	The focus on cloud manufacturing means direct applicability to voting systems may require significant adaptation.	To demonstrate blockchain's ability to enforce agreements and ensure accountability, principles that can enhance trust in voting systems.
13.	A Study on Public Blockchain Consensus Algorithms: A Systematic Literature Review.	This study reviews public blockchain consensus algorithms, examining their characteristics, advantages, and limitations.	The paper does not focus directly on voting systems, requiring extrapolation to apply findings to voting contexts.	This helps to understand consensus mechanisms underpinning blockchain
14.	Blockchain and Cryptocurrencies	This article explores blockchain and cryptocurrencies, discussing	The financial focus limits direct relevance to voting systems without	To gain insights into blockchain's broader applications for

		blockchain's applications beyond finance and implications for risk management.	contextual adaptation.	to voting systems.
15.	E-voting scan integrity: End-to-end voter verifiable optical scan voting. IEEE	This article discusses end-to-end verifiable optical-scan voting, focusing on maintaining process integrity through cryptographic protocols.	The paper predates modern blockchain applications, requiring integration of contemporary blockchain advancements.	This motivates to ensure transparency and trustworthiness in voting.

Table 2.1 Review on Literature Survey

CHAPTER 3

PROBLEM DEFINITION AND OBJECTIVES

3.1 PROBLEM DEFINITION

- In contemporary democratic systems, traditional voting methodologies suffer from critical flaws such as susceptibility to manipulation, lack of transparency, and vulnerability to fraud.
- These deficiencies undermine the sanctity of the electoral process, compromising the integrity of democratic decision-making.
- To address these issues, the Execution of a blockchain technology-based voting system emerges as a viable solution. Blockchain technology offers inherent features like immutability, transparency, and decentralization, which can potentially revolutionize the electoral process, ensuring trust, security, and inclusivity
- This project seeks to enhance security and transparency by integrating blockchain technology and face recognition into the existing e-voting infrastructure.

The goal is to mitigate manipulation and unauthorized access, ensuring the Reliability of e-voting in democratic processes. ethical concerns such as misinformation or misuse, poses a significant problem. Lack of security and consensus protocol.

3.2 OBJECTIVES

- **Strengthening Security Against Unauthorized Access and Manipulation:**

  Implement robust authentication mechanisms such as multi-factor authentication (MFA) and digital signatures to ensure only authorized individuals can access the voting system. Employ encryption techniques to secure data transmission and storage, preventing unauthorized tampering or interception of votes. Utilize blockchain's immutable ledger to record and timestamp each vote, making it practically impossible for malicious actors to alter or delete votes without detection

- **Improving Vote Tallying Speed:** Employ optimized algorithms and consensus mechanisms within the blockchain network to expedite the process of vote counting and validation. Utilize parallel processing or sharding techniques to divide the workload, enabling simultaneous tallying of votes to significantly reduce processing time.

- **Enhancing System's Scalability for Handling Large Vote Volumes:** Design a scalable infrastructure that can accommodate a high volume of votes by leveraging features such as off-chain processing or layer 2 solutions while maintaining the security and integrity of on-chain data. Implement load balancing techniques to distribute incoming vote requests efficiently across multiple nodes or servers, ensuring smooth operations during peak voting periods.

- **Creating Standardized Protocols for Secure Electronic Voting:** Develop a comprehensive set of standardized protocols that encompass encryption standards, verification processes, and data integrity checks, ensuring a consistent and secure voting experience across different jurisdictions. Collaborate with international standards bodies or electoral commissions to establish universally accepted protocols for secure electronic voting, fostering trust and reliability in the system.

- **Ensuring Voter Privacy and Anonymity:** Implement cryptographic techniques within the blockchain system to guarantee the confidentiality of individual votes. Explore zero-knowledge proofs or homomorphic encryption to enable the verification of votes without revealing specific voter choices. Prioritize the development of protocols that uphold the principle of secret ballot while leveraging the transparency benefits of blockchain technology.

- **Promoting Accessibility and Inclusivity:** Design the blockchain technology-based e-voting system with user-friendly interfaces to ensure accessibility for individuals with diverse technological literacy levels. Consider the implementation of mobile voting applications and accessible interfaces for voters with disabilities. Collaborate with accessibility experts to address the unique needs of different voter demographics, promoting inclusivity in the electoral process.

- **Decreasing Operational Expenses Associated with Traditional Voting:** Conduct a cost-benefit analysis comparing the expenses incurred in implementing and maintaining the blockchain-based e-voting system against traditional voting methods.Highlight the potential cost savings achieved through reduced manual labor, paper usage, transportation, and logistical overheads associated with traditional voting, emphasizing the efficiency gains.

- **Integrating Accessibility to Remote and Overseas Voters:** Explore innovative solutions, such as blockchain-powered mobile voting apps or secure online platforms, to facilitate remote voting for citizens residing abroad or in geographically remote areas. Collaborate with international organizations and diplomatic missions to implement secure methods for overseas voters, ensuring their participation in the election process while maintaining the same level of Safety and integrity as on-site voting.

CHAPTER 4

SYSTEM REQUIREMENTS AND SPECIFICATION

4.1 SOFTWARE REQUIREMENTS

- Programming Language for smart contract: Solidity
- Development IDE: Visual Studio Code
- Database: MySQL
- Frontend: Html, CSS, JavaScript,
- Backend: Python, Ganache

4.1.1 Visual Studio

Visual Studio is an integrated development environment (IDE) created by Microsoft. It is primarily used for developing computer programs, websites, web applications, and mobile apps. Visual Studio provides a comprehensive set of tools for coding, debugging, testing, and deploying applications across a variety of platforms, including Windows, macOS, iOS, Android, and web browsers.

4.1.2 Ganache

Ganache is a personal blockchain for Ethereum development. It is primarily used by developers to test their Ethereum smart contracts and Decentralized Applications (DApps) in a local development environment. Ganache provides a simulated blockchain network that runs locally on our machine, allowing developers to interact with it as if it were a real Ethereum network, but without the overhead or cost associated with deploying to a public blockchain.

Sl. No.	Software Name	Description	Version	RAM Required	Memory Required
01	Android Studio	IDE used For Coding	Visual Studio 17.9	4 GB	20 GB
02	Ganache	Used to Create Personal blockchain environment	Ganache 7.9.2	4 GB	20 GB

Table 4.1 Software Toolset

4.2 HARDWARE REQUIREMENTS

- Processor: Intel Core i5 10th Gen
- Speed: 1.6 Ghz (minimum)
- RAM: 4 Gigabyte (minimum)
- Memory: 200 Megabyte (minimum)

4.3 Software requirements for User

- Windows 7 or higher OS
- Google chrome or any other safe browser
- Internet Speed minimum 2 mbps

4.4 Hardware Requirements for User

- Any mobile or PC/Laptop containing camera with min 4GB ram.

CHAPTER 5

SYSTEM DESIGN

5.1 USE CASE DIAGRAM

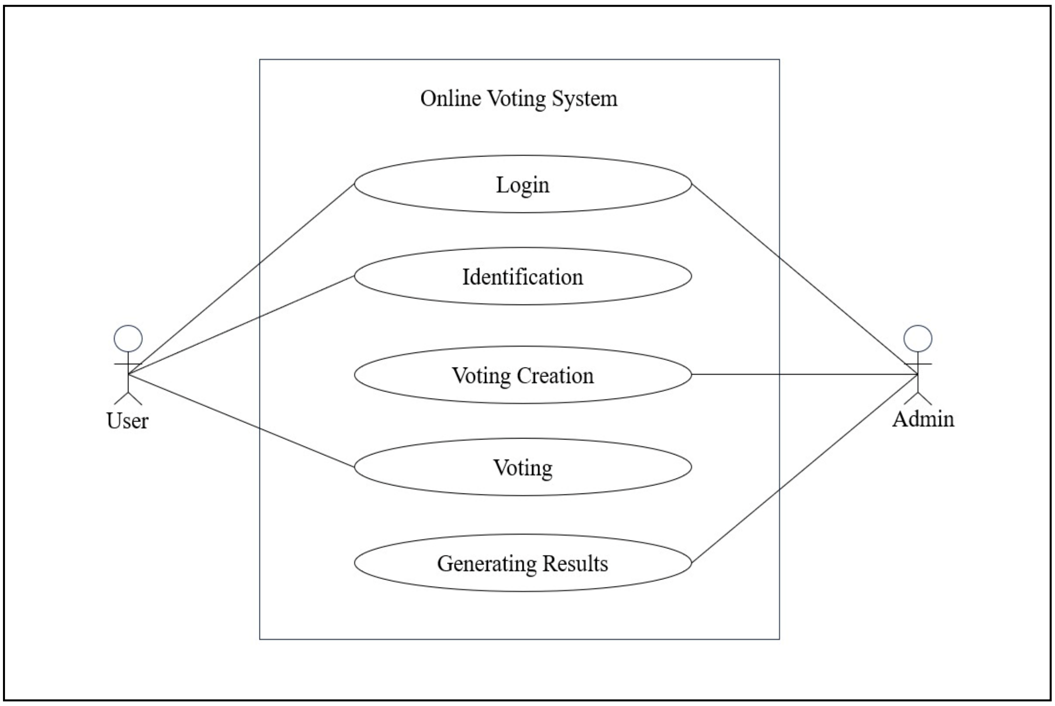

Figure 5.1 Use-Case Diagram

Use case diagrams are a common way to communicate the major functions of a software system. A use case diagram provides a simplified illustration of how users interact with a system, displaying the relationship between users and the various use cases they engage with. It identifies different types of users and the specific use cases they participate in. Typically, a use case diagram is complemented by other types of diagrams to provide a comprehensive understanding of the system's functionality and user interactions.

Use cases are nothing but the system functionalities written in an organized manner. Nowanother thing which is relevant to the use cases are the actors. Actors can be defined assomething that interacts with the system.

5.2 FLOW CHART

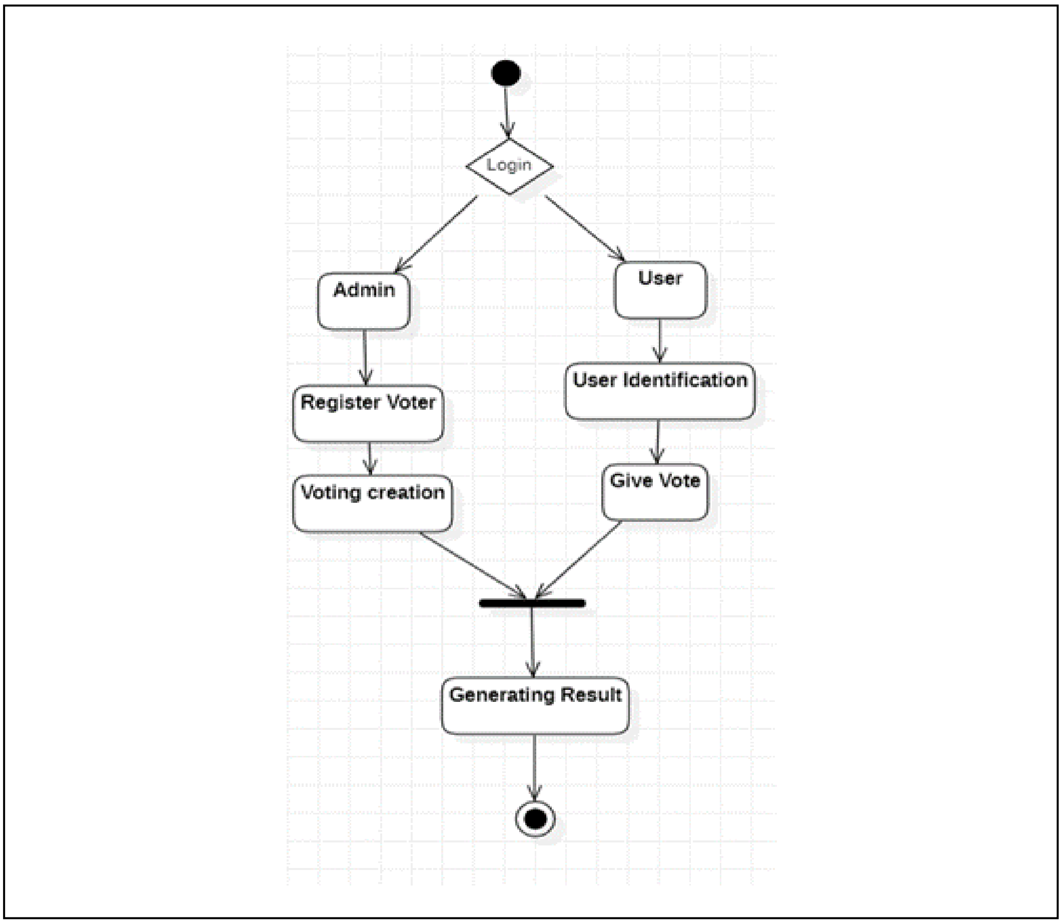

Figure 5.2 Flow Chart

Start Application: The flow diagram begins when the application is launched, either on a mobile device or a computer.

Voter Registration: During registration, voters provide their unique ID number, email address, name, and phone number. The system utilizes facial recognition technology for login purposes, requiring a clear video selfie at signup.

Login and Authentication: Following registration, voters log in using a password. Successful login is followed by facial recognition for boosting security and real-time authentication.

Blockchain for Secure Voting*:* The system leverages blockchain technology for its inherent security and transparency. Blockchain encrypts cast votes using an asymmetric encryption algorithm. The public key for verification resides on the blockchain, while the private key is held by the system.

Ethereum for Transaction Execution*:* The Ethereum network serves as the framework for creating and storing the blockchain. Encrypted blocks containing voting data is distributed across numerous nodes, ensuring system resilience. Voters interact with smart contracts on a private Ethereum blockchain environment created using Ganache to cast their votes.

Admin Role and Responsibilities: The administrator manages the entire voting platform. This includes verifying voter and candidate registrations, scheduling elections, and controlling crucial notifications, such as results announcements.

Results Processing and Transparency: The results stage involves vote tabulation and generation. The system displays the outcome on the website. Voters can identify their votes using their public keys, upholding the system's transparency.

End: Once the Vote have been initiated, the flow diagram reaches its end. The application remains active, ready to respond to any further user actions.

5.3 DATA FLOW DIAGRAM

5.3.1 LEVEL 0 DFD

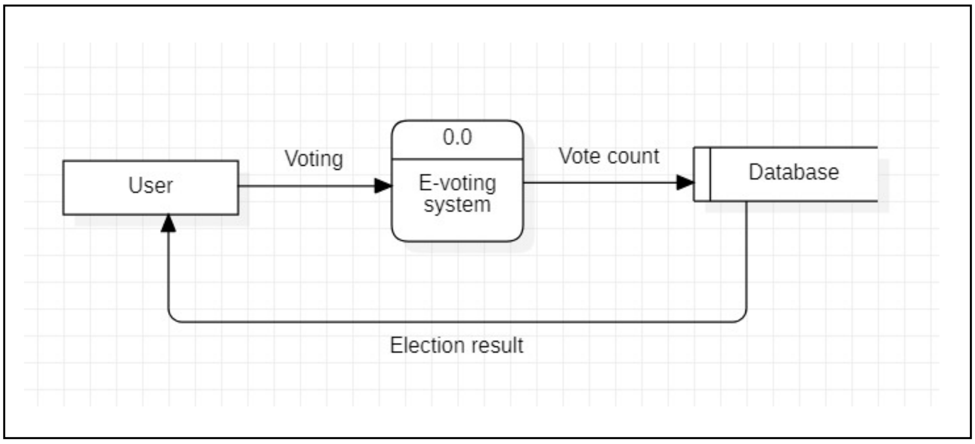

Figure 5.3.1 Level 0 DFD

A Level 0 Data Flow Diagram (DFD) is a simplified graphical representation that illustrates the flow of data between a system and external entities. The Level 0 DFD serves as a foundational starting point for requirements analysis and system design, helping stakeholders grasp the data flow and interactions between the system and its external counterparts.

5.3.2 LEVEL 1 DFD

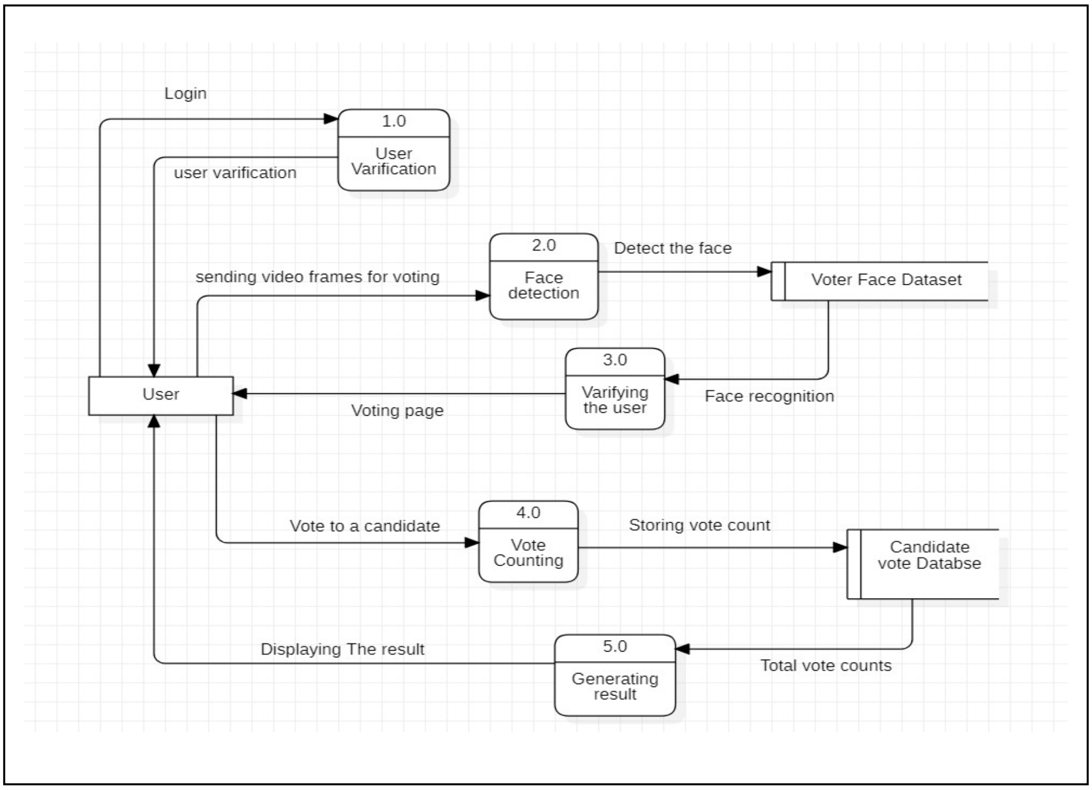

Figure 5.3.2 Level 1 DFD

A Level 1 Data Flow Diagram (DFD) is a more detailed representation of the system's processes, data flows, and interactions with external entities compared to the Level 0 DFD. It provides a more granular view of how data moves within the system and between different processes. The Level 1 DFD expands on the processes identified in the Level 0 DFD and breaks them down into sub-processes or modules, illustrating the inputs, outputs, and data transformations at a more specific level.

5.4 SEQUENCE DIAGRAM

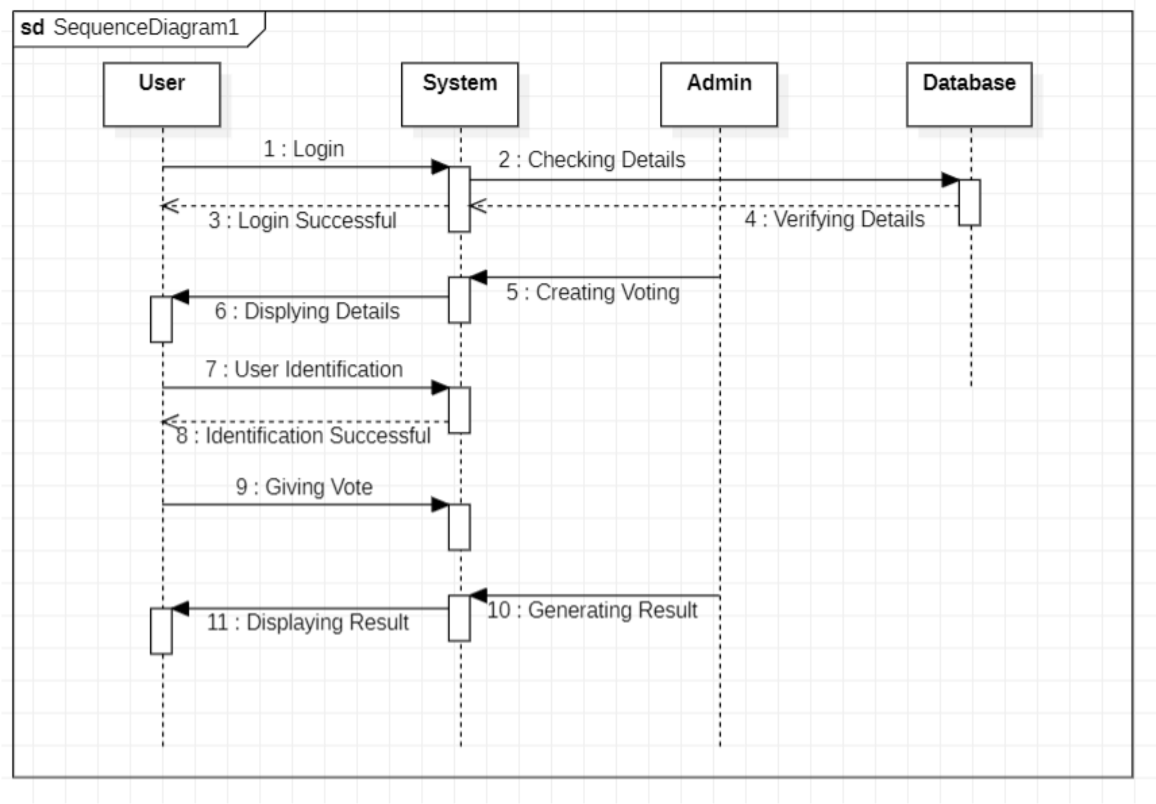

Figure 5.4 Sequence Diagram

A sequence diagram visually represents the behavioural aspects of a system, depicting interactions between objects through the passing of messages over time. It consists of objects within the system, their lifelines, and the messages exchanged between them.

Objects are depicted at the top of the sequence diagram within rectangular boxes. Each object is labelled with its name followed by a colon and the class name from which it is instantiated. The entire string is underlined and enclosed within a rectangle box. A downward vertical line extending from the object box represents the object's lifeline. A rectangular bar along the lifeline indicates the object's activity at a specific point in time.

Messages between objects are depicted as arrows extending from the lifeline of the sending object to the lifeline of the receiving object. The arrow is labelled with the message name, indicating the communication between the objects.

5.5 ACTIVITY DIAGRAM

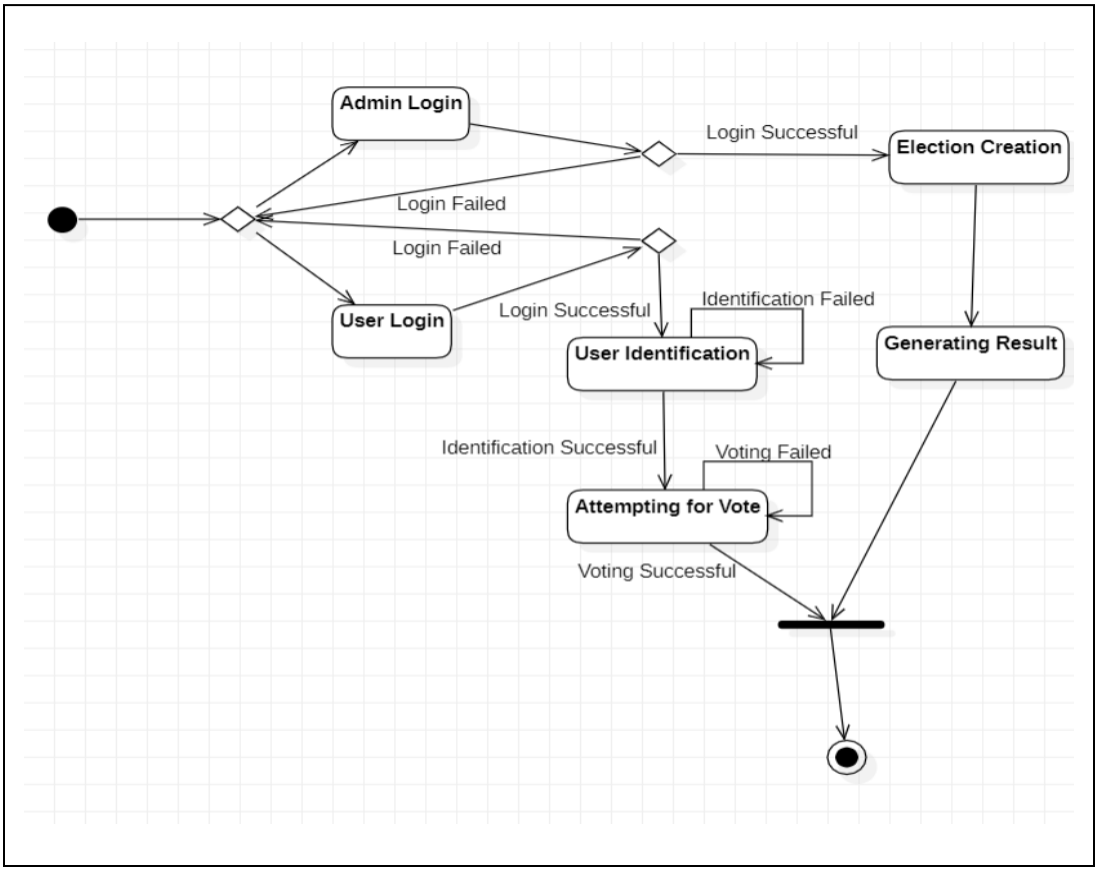

Figure 5.5 Activity Diagram

An activity diagram is a visual representation that illustrates the flow of activities or processes within a system, showcasing the sequential order and decision points. It helps in understanding the workflow, business processes, and interactions between different elements of a system. Activity diagrams are valuable tools for analyzing, documenting, and improving system processes and can be utilized in various domains such as software development, business process modeling, and project management.

5.6 ARCHITECTURE DIAGRAM

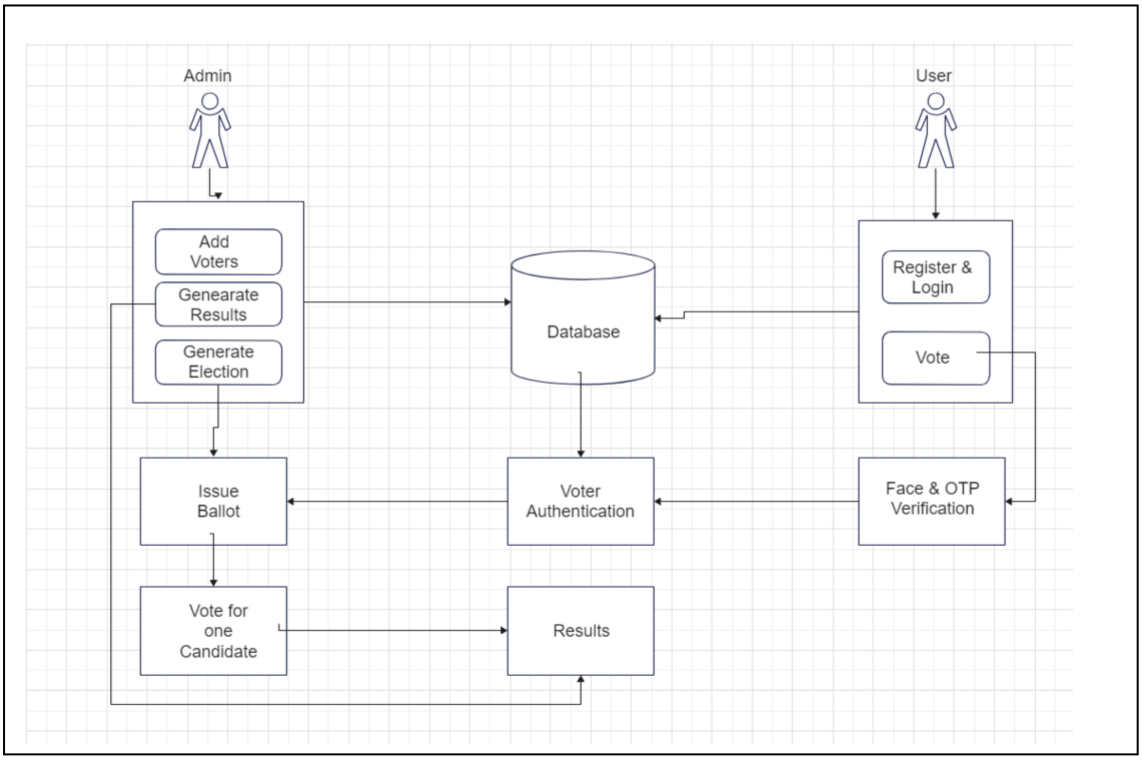

Figure 5.6 Architecture Diagram

- **Voter Registration:** During registration, voters provide their unique ID number, email address, name, and phone number. The system utilizes facial recognition technology for login purposes, requiring a clear video selfie at signup.

- **Login and Authentication:** Following registration, voters log in using a password. Successful login is followed by facial recognition for boosting security and real-time authentication.

- **Blockchain for Secure Voting:** The system leverages blockchain technology for its inherent security and transparency. Blockchain encrypts cast votes using an asymmetric encryption algorithm. The public key for verification resides on the blockchain, while the private key is held by the system.

- **Ethereum for Transaction Execution:** The Ethereum network serves as the framework for creating and storing the blockchain. Encrypted blocks containing voting data is distributed across numerous nodes, ensuring system resilience.

Voters interact with smart contracts on a private Ethereum blockchain environment created using Ganache to cast their votes.

- **Results Processing and Transparency:** The results stage involves vote tabulation and generation. The system displays the outcome on the website. Voters can identify their votes using their public keys, upholding the system's transparency.

CHAPTER 6

IMPLEMENTATION

6.1 Voting Process:

Here, we outline a typical user interaction within the proposed scheme based on our current system implementation. The voter initiates the process by logging into the system using Adhaar Id, Password and facial recognition. Upon scanning their face, the facial recognition system authenticates the voter. If a successful match is found, the voter is Showcased with a catalog of available candidates and the option to vote for or against them. Conversely, if the match fails, further access is denied. This functionality is facilitated by an appropriate implementation of an authentication mechanism (in this case, facial recognition) and predefined role-based access control.

It is assumed that each voter is assigned to their respective electoral district, and this information is utilized to generate a list of candidates eligible for the voter's Assortment. The process of assigning voters to constituencies is considered offline and falls beyond the scope of this research.

Once a vote is successfully cast, it undergoes verification by multiple miners. Valid and verified votes are then added to the public ledger. Security measures are based on blockchain technology, utilizing cryptographic hashes for end-to-end verification. A successfully cast vote is treated as a transaction within the voting application's blockchain, resulting in its addition as a new block upon successful mining. Additionally, the vote is stored in the database's data tables.

The system ensures that each person has ownership of only one vote. This is ensured by matching the unique voter face at the beginning of each voting attempt to prevent double voting. Upon mining a vote, a unique transaction is generated for each vote. Malicious votes are rejected during the validation process.

Following validation, a notification containing the transaction ID is promptly sent to the voter via message or email. This allows the user to track their vote on the ledger. While serving as a voter notification mechanism, this process does not reveal how a specific voter cast their vote, thus preserving voter privacy.

6.2 Overview of the system:

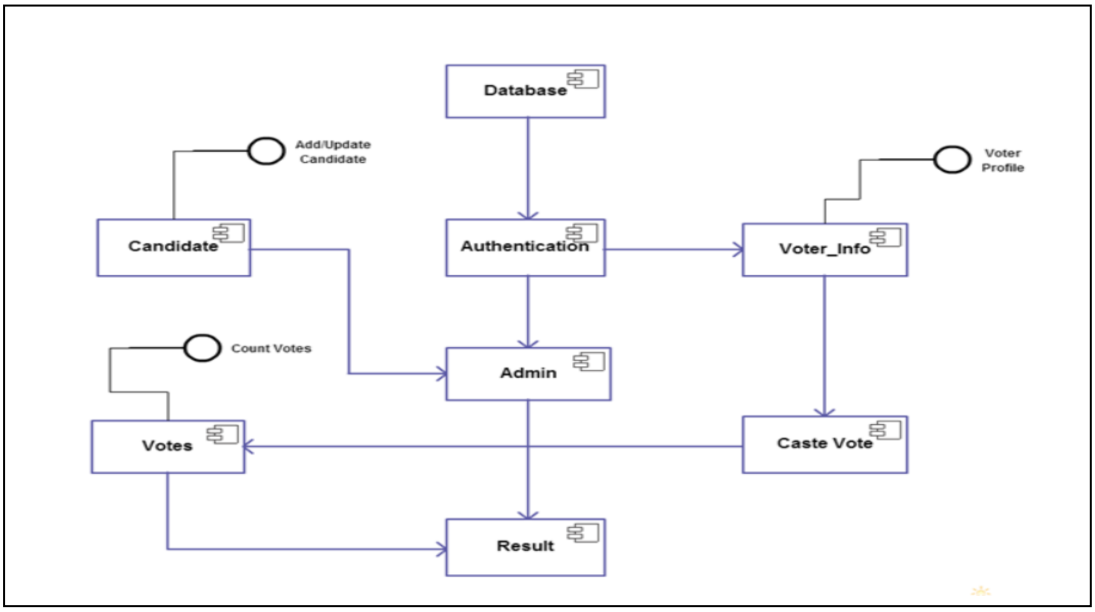

Figure 6.1 Overview of system

- The proposed system offers a streamlined and secure method for voter interaction, enhancing the efficiency and accessibility of the voting process. Upon logging into the system, voters undergo facial recognition authentication, granting access to the list of candidates relevant to their electoral district. This authentication mechanism, coupled with role-based access control, ensures that only authorized individuals can participate in the voting process.
- Once a voter selects their preferred candidate, their vote is mined by multiple miners for verification. Valid votes are then added to the public ledger, secured through blockchain technology utilizing cryptographic hashes for end-to-end verification. Each successfully cast vote is treated as a transaction within the blockchain, recorded both as a new block and in the database. This approach ensures the integrity of the voting system, preventing duplicate votes through the use of unique facial recognition identifiers.
- Following validation, voters receive immediate notification of their transaction ID via message or email, allowing them to track their vote on the ledger. While this notification provides transparency, it maintains voter privacy by safeguarding individual voting choices. Each voter's identity is represented by a cryptographic

hash within the blockchain, ensuring anonymity even from system operators or administrators.

- By leveraging blockchain technology and robust authentication mechanisms, the proposed system offers a comprehensive solution to enhance the integrity and accessibility of the voting process. Its emphasis on security, privacy, and verifiability ensures a fair and transparent electoral system, addressing the shortcomings of traditional voting methods.

6.3 Working of the System:

Registration Stage: During this stage, the voter is required to register using their unique Aadhar number, email address, name, and phone number. Additionally, they must upload a clear photo since the system employs facial recognition technology for authentication.

Login: Following registration, the voter attempts to log in to cast their vote. Initially, they log in using a password. Upon successful login, the voter must authenticate themselves further to vote. Real-time authentication is achieved through facial recognition technology, heightening the level of security.

Blockchain Technology: This technology is primarily utilized for its security features. Blockchain ensures a secure and transparent environment by encrypting the voter's message (i.e., casted vote) using an asymmetric encryption algorithm. The public key is provided by the Blockchain, while the private key remains with the host. The public key serves authentication purposes using the ledger.

Ethereum: The Ethereum network offers a framework for creating and storing the blockchain. Each block is created and its details are stored in an encrypted ledger. These blocks are then distributed among the nodes, enhancing the system's fault tolerance. To cast a vote, users must conduct transactions using Ethereum. Ganache, a private blockchain environment Ethereum, is employed for this purpose. It enables users to emulate the Ethereum blockchain and interact with smart contracts on a private blockchain.

Database: All system data is stored in the MongoDB database. This data includes voter and candidate names, unique voter IDs, and voting details such as time, time slot, and region.

Admin: The admin has control over the entire environment. They are responsible for verifying voters and candidates, arranging the voting schedule, and managing important notifications such as results.

Results Phase: The processing and counting of votes occur during this phase. The results are generated and displayed on the website. Users can Authenticate their casted votes using their public key, ensuring transparency within the voting system.

6.4 Blockchain

6.4.1 Introduction

Blockchain technology has risen to prominence, particularly with the advent and widespread adoption of Bitcoin, the very first cryptocurrency to capture public attention. Originating from the underlying architecture of Bitcoin, blockchain technology quickly emerged as a promising innovation due to its high level of transparency within the system, leading to extensive research and exploration of its various applications across different fields.

In essence, blockchain serves as a shared and immutable ledger, facilitating the recording of transactions and tracking of assets within a business network. These assets can be tangible, such as real estate, vehicles, or currency, or intangible, including intellectual property, patents, copyrights, and branding. In today's era, almost anything can be tracked and traded on a blockchain network, resulting in reduced costs and risks for all parties involved.

Blockchain organizes its data into blocks, with each block containing smaller components of the information allocated across a decentralized network. The initial block in a blockchain is commonly referred to as the "Genesis Block" or "Block 0." This genesis block holds a special significance as it is typically hard-coded into the software and lacks a reference to a previous block.

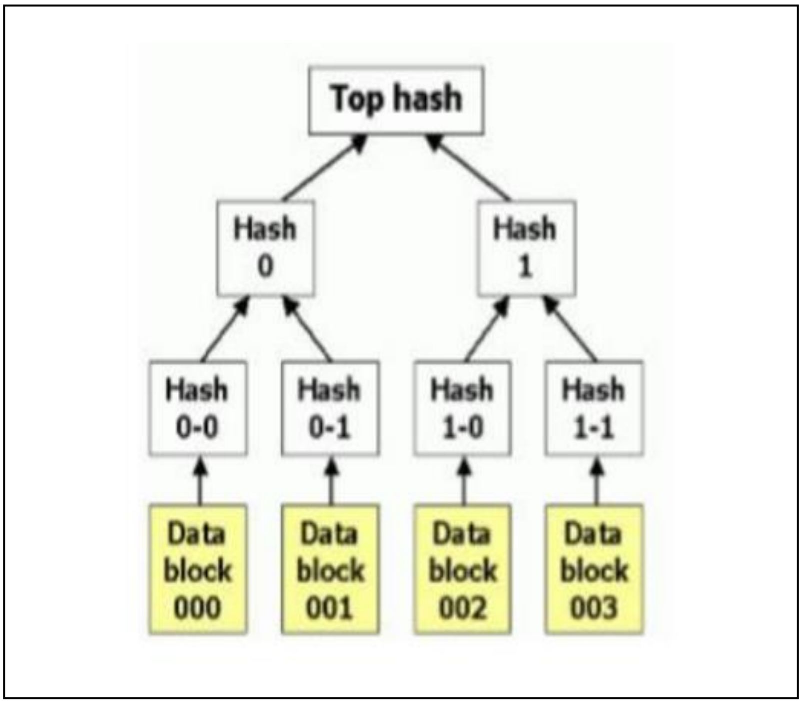

Figure 6.2 Bitcoin Hash Block

After the genesis block is initialized, subsequent blocks are created, with "Block 1" being the first one generated. Each block contains a transaction data section, where copies of transactions are hashed and then these hashes are iteratively combined and hashed again until only one hash remains, known as the Merkle root. The Merkle root is stored in the block header, ensuring that transactions cannot be tampered with by third parties.

Blockchain operates on a peer-to-peer network architecture, where each node communicates with other nodes to exchange blocks and transactions. A blockchain block comprises a block header, a hash value of the previous block header, and a Merkle root. When extracting data from the blockchain, all the smaller parts distributed across the decentralized network are connected by accessing all the blocks through their hash values. To alter the data, a person or third party would need to know the hash values of all the blocks. Without this information, they cannot access any part of the data. Since data blocks are dispersed across thousands of blocks, it would take a hacker millions of years to uncover all the hash values. These features ensure the safety, reliability, and robustness of blockchain technology.

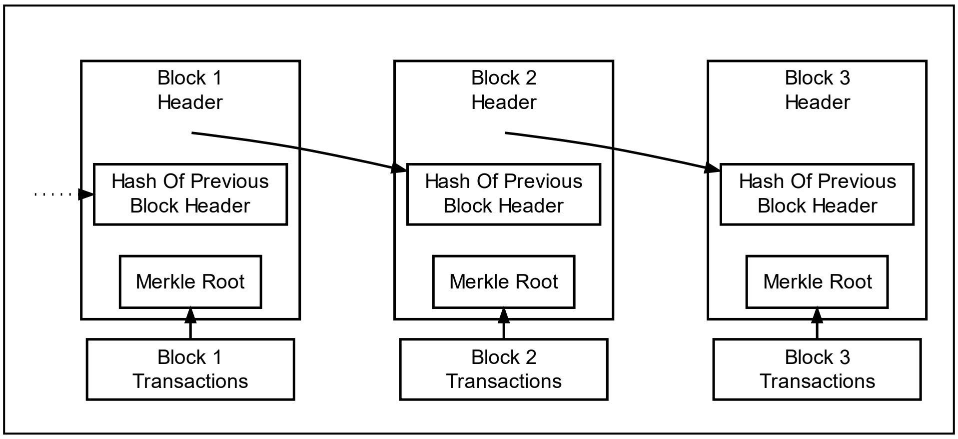

Figure 6.3 Simplified Bitcoin Blockchain

Before 2004, India relied on a paper-based voting system known as the ballot paper system. To address the shortcomings of traditional voting methods, blockchain emerges as a fitting solution for an electronic voting platform. While electronic voting has been extensively studied and implemented, challenges such as user authentication and vote tampering have been encountered. Unlike other government websites or platforms for information dissemination, online elections require heightened security, reliability, and authenticity due to the significance of each vote in determining elected officials—a cornerstone of democracy and democratic governance, which is widely fevered in the modern world. Transitioning to an electronic voting system presents several advantages. It simplifies the voting process, making it more accessible to voters, prioritizes security, and reduces costs associated with traditional voting methods. Additionally, it addresses issues like long queues at polling stations and provides convenience for individuals who are ill, serving in the military, residing abroad, or on vacation. Moreover, electronic voting can motivate individuals who may have abstained from voting due to laziness or inconvenience.

In today's digitized world, the electoral system must keep pace with technological advancements. Leveraging the internet can help engage young voters aged 18 to 30, who may be challenging to reach through traditional means. By embracing electronic voting, the electoral system can modernize and adapt to the preferences and behaviors of contemporary society.

Our main provocation behind this design is to produce a secure voting terrain and show that a dependablee-voting scheme is possible using blockchain. Because when electronic voting is available to anyone with a computer or mobile phone, every single executive decision can be made by people and members; or at least people's opinions will be more public and accessible to politicians and directors. This will ultimately lead humanity to true direct republic. This is important to us because choices can be fluently corrupted or outfitted, especially in small municipalities and indeed larger metropolises in loose countries. also, large- scale traditional choices are veritably precious in the long run, especially when there are hundreds of geographically distributed polling stations and millions of choosers. Voter turnout at polling stations is also fairly low, as the person may not be staying at the address whose name is on the list, or perhaps on holiday or other work. Electronic voting will be suitable to break these problems if enforced precisely. The conception of electronic voting is significantly aged than blockchain. So, all known exemplifications to date have used the means of centralized computing and storehouse models. By enforcing blockchain, we can increase the security position of our system due to its way of storing data in a decentralized network. This design also has a facial recognition system to corroborate whether the stoner is valid or not. Some systems were set up to have an OTP system to authenticate the stoner. But in this authentication model, the disadvantage is that if x person's phone isn't with him, indeed though his phone is with his friend, his friend can bounce doubly because of the OTP system, one with the original chance and one because of his friend's login, and also x cannot bounce. So then comes the face recognition fashion where the stoner has to corroborate his face before advancing to maintain translucency.

6.4.2 Solidity

Solidity is an object-oriented, high-level programming language utilized for crafting smart contracts that automate transactions on the blockchain. Initially proposed in 2014, Solidity was developed by contributors to the Ethereum project, predominantly for creating smart contracts on the Ethereum blockchain, although it can be employed for other blockchain platforms as well.

The language bears similarities to JavaScript, a widely-used programming language, and can be regarded as a dialect of JavaScript. This implies that individuals familiar with JavaScript may find it relatively straightforward to grasp Solidity. Additionally, Solidity shares resemblances with programming languages such as C++ and Python.

As a high-level language, Solidity eliminates the need for coding in binary format (ones and zeros), making it more accessible for humans to write programs using a combination of letters and numbers, which are easier to comprehend.

Solidity is statically typed and supports features such as inheritance, libraries, and complex user-defined types. Static typing necessitates specifying each variable and enables the compiler to verify the correct usage of variables. Solidity data types are typically categorized as value types or reference types.

The distinction between value types and reference types lies in how they are assigned to variables and stored in the Ethereum Virtual Machine (EVM). Altering the value in one variable of a value type does not impact the value in another variable, whereas updates to reference type variables can affect other variables referencing the modified values.

Figure 6.4 Working of Solidity

6.4.3 Metamask

MetaMask is a cryptocurrency wallet available as a browser extension, designed to aid users in storing tokens, interacting with decentralized applications, and trading Ethereum. By integrating with My Ether Wallet, MetaMask streamlines transactions by eliminating the need to input private keys for each transaction, whether creating, storing, or trading tokens.

Users can utilize MetaMask to store and manage various cryptocurrencies, including Bitcoin and Ether, through a blockchain wallet accessible digitally or online. A blockchain wallet facilitates cryptocurrency transfers, safeguards against theft of crypto assets, and enables users to convert them into local currencies if required. Boasting a robust community with over a million downloads, MetaMask benefits from numerous resources contributing to its ongoing development and improvement.

The MetaMask browser extension serves as an Ethereum wallet, offering the convenience of not requiring additional plug-ins, thus allowing users to employ it across various browsers. Once installed, users can access their Ethereum address, send or receive coins to any Ethereum address, and engage in various activities such as staking coins on gambling sites, trading on decentralized exchanges (DEXs), and participating in projects like Pool Together and Compound.

6.4.4 Ganache

Ganache is a tool that enables users to create their own local Ethereum blockchain. This blockchain can be employed across all stages of the development process, rendering Ganache a highly valuable tool. By facilitating the setup of a local blockchain, Ganache empowers users to deploy, develop, and test all their Decentralized Applications (dApps) within a secure and deterministic environment.

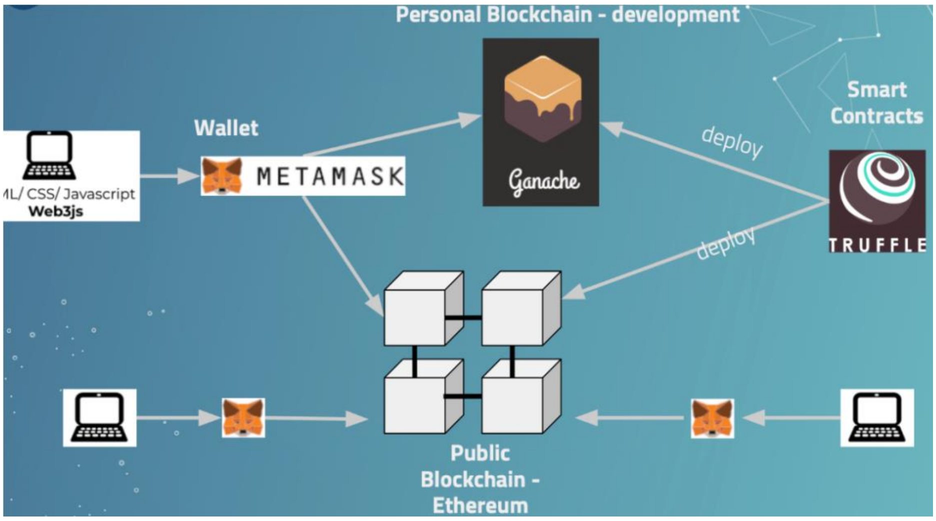

Figure 6.5 Blockchain Transaction Flow

6.4.5 Face Recognition

User identification is performed using the face recognition technique. Before casting a vote for any candidate, the user must authenticate themselves through face recognition. This ensures the reliability of the voting process by verifying that the individual casting the vote is authorized, preventing unauthorized voting by others.

The face recognition functionality is implemented using the world's simplest face recognition library, which can be accessed from Python or through the command line interface. This library is built using dlib's cutting-edge face recognition technology, which utilizes deep learning. With an impressive accuracy rate of 99.38% on the Labeled Faces in the Wild benchmark, this library provides a straightforward face recognition command line tool that allows users to perform face recognition.

CHAPTER 7

TEST CASES

Test Case 1:

Form Name	Login
Test Data	User Id, Password
Input	Login and Password
Expected Result	User should not be able to login without proper authorization.
Actual Result	User cannot access voting or admin page without authorization.
Result	Passed

Table 7.1 Test Case 1 Login

Test Case 2:

Form Name	Verify user login
Test Data	Button Clicks, Application
Input	Voter id and password
Expected Result	User is able to login with correct credentials only
Actual Result	Worked as expected
Result	Passed

Table 7.2 Test Case 2 Verify User Login

Test Case 3:

Form Name	Registration
Test Data	Full name, Age, Gender, Email Id, password, Mobile number, address
Input	Full name, Age, Gender, Email Id, password, Mobile, address And click on Register button
Expected Result	Check for all valid inputs and registers a new user
Actual Result	Worked as Expected
Result	Passed

Table 7.3 Test Case 3 Registration

Test Case 4:

Form Name	Login
Test Data	voter id, password
Input	voter id=” DEEBGM123”, password=” Deepak123” And click on Sign In button
Expected Result	Check for Login id, password. If login id or the password or both not entered display message
Actual Result	Worked as Expected
Result	Passed

Table 7.4 Test Case 4 Voter Login

Test Case 5:

Form Name	OTP Authentication
Test Data	OTP Generation and Authentication
Input	Valid mobile number or email address for OTP delivery. Invalid mobile number or email address format.
Expected Result	The system should generate OTPs correctly and send them to the provided mobile number or email address
Actual Result	OTPs are generated and delivered correctly.
Result	Passed

Table 7.5 Test Case 5 OTP Authentication

Test Case 6:

Form Name	Verify candidate registration
Test Data	Candidate name and party.
Input	Candidate name and party.
Expected Result	Registration transaction should be successful.
Actual Result	Worked as expected
Result	Passed

Table 7.6 Test Case 6 Verify candidate Registration

Test Case 7:

Form Name	Verify date registration
Test Data	Starting and ending date
Input	Starting and ending date
Expected Result	Date transaction should be successful.
Actual Result	Worked as expected
Result	Passed

Table 7.7 Test Case 7 Verify date registration

Test Case 8:

Form Name	Facial Recognition Authentication
Test Data	Face Recognition Accuracy
Input	Different lighting conditions (bright, dim, low light), various facial expressions (neutral, smiling, frowning), different angles (frontal, profile), and different distances from the camera.
Expected Result	The system should accurately identify registered users under different lighting conditions, facial expressions, angles, and distances. Upon successful recognition, the system should grant access to the user.
Actual Result	Struggles to detect faces in poor lighting conditions.
Result	Passed

Table 7.8 Test Case 8 Face Recognition Authentication

Test Case 9:

Form Name	Verify voting
Test Data	Candidate names
Input	Select a candidate and click “Vote” button
Expected Result	Vote transaction should be successful.
Actual Result	Vote transaction is successful.
Result	Passed

Table 7.9 Test Case 9 Verify voting

CHAPTER 8:

RESULTS AND ANALYSIS

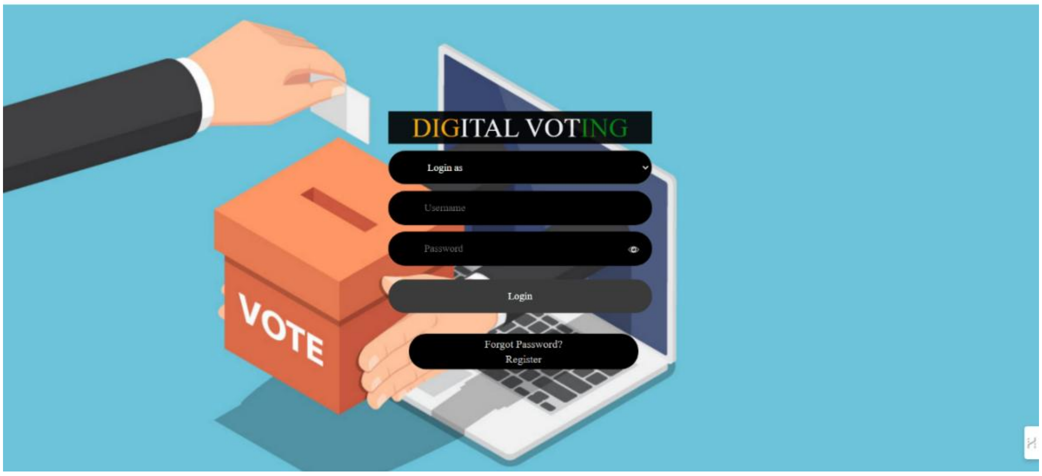

Figure 8.1 Login Page

The login page serves as the gateway for users to access the voting system, ensuring secure authentication and user verification.

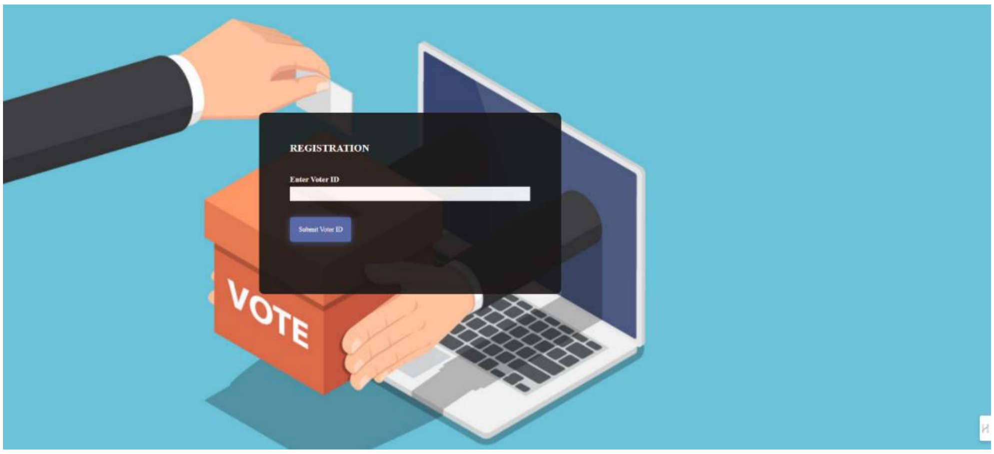

Figure 8.2 Voter Registration

The voter registration page facilitates the enrollment process for individuals to participate in the voting system using voter id and collecting necessary information.

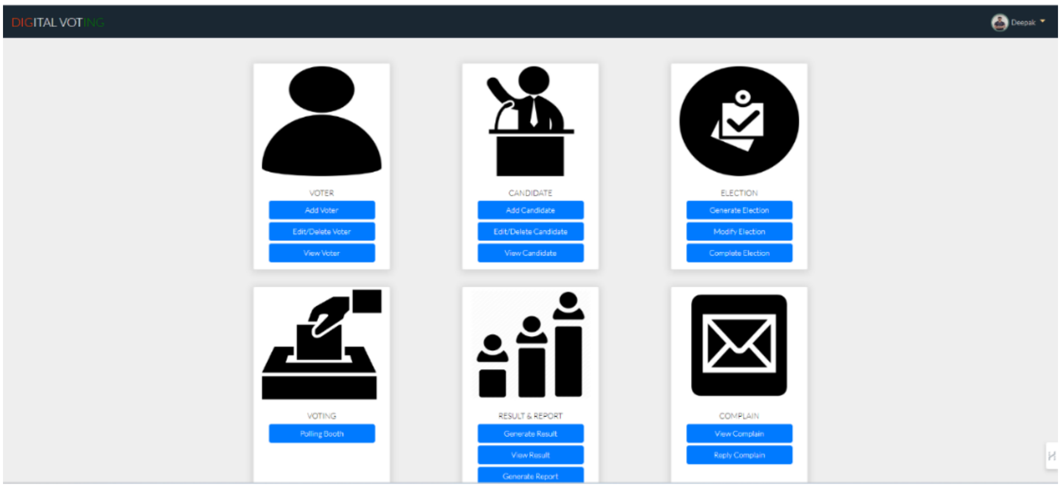

Figure 8.3 Admin Panel

The admin panel provides authorized personnel with a centralized interface to manage and oversee various aspects such as adding voter, election generation, add candidate, view complain.

Figure 8.4 Add Candidate

The Add Candidate feature allows administrators to securely input and store candidate information into the voting system.

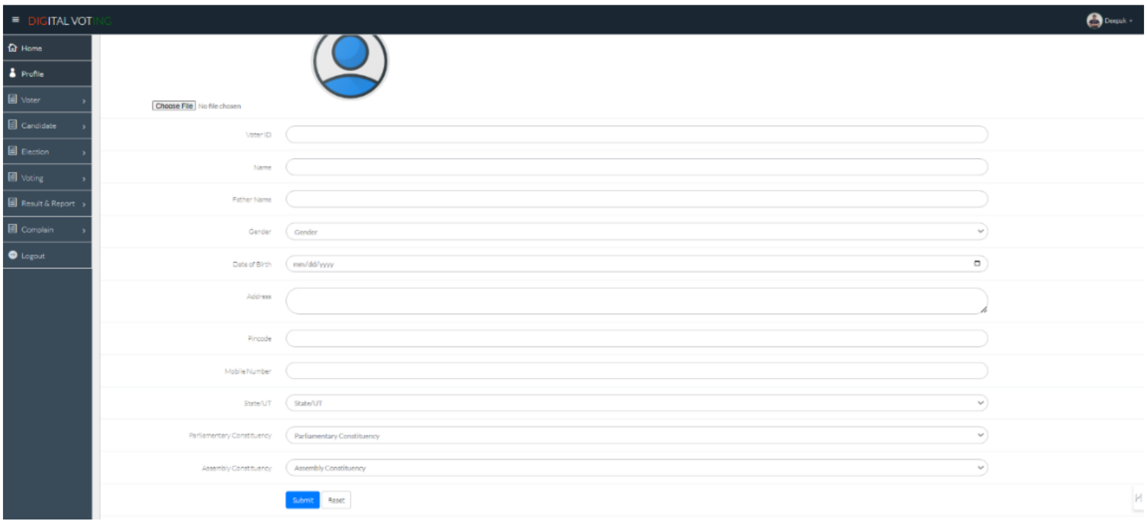

Figure 8.5 Add Voter

The Add Voter function enables administrators to securely register new voters into the system.

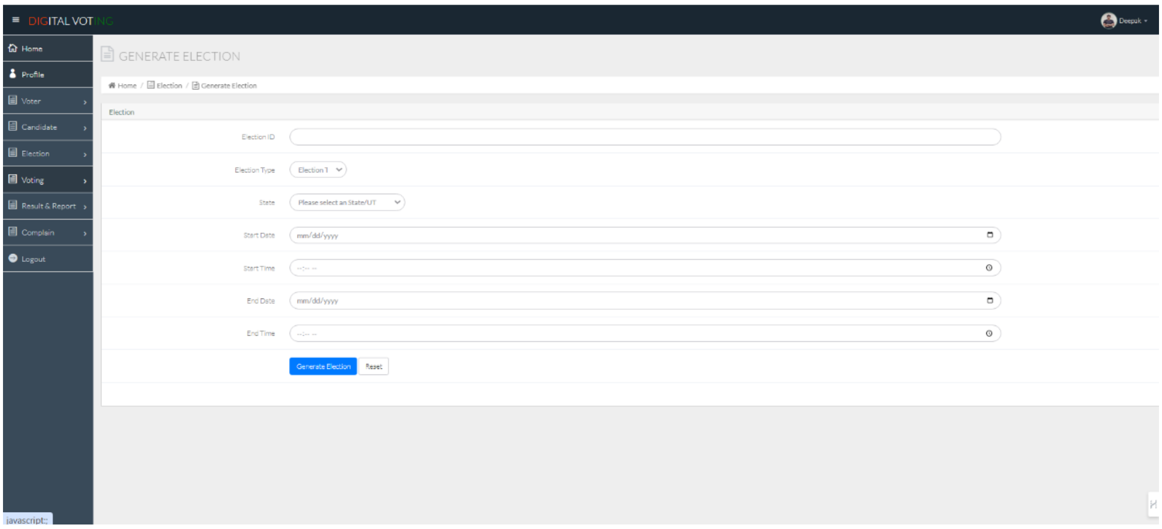

Figure 8.6 Election Generation

The admin can generate election by selecting consticency ,start date-time and end date-time.

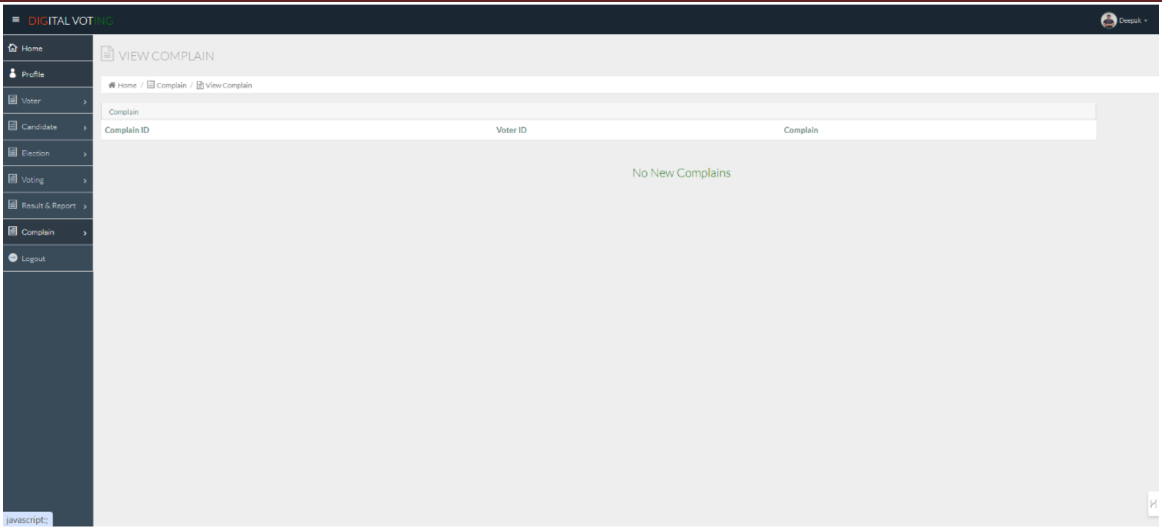

Figure 8.7 Complain View

The Complain View section provides a platform for users to submit and view complaints.

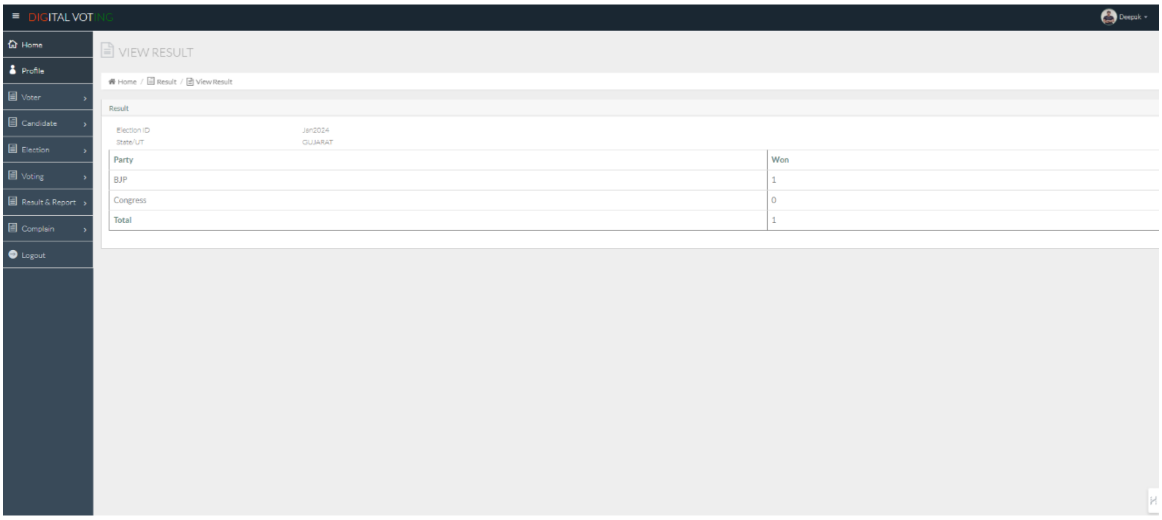

Figure 8.8 View Election Result

The View Election Result feature allows users to access and review the outcome of elections, promoting transparency and trust in the voting system.

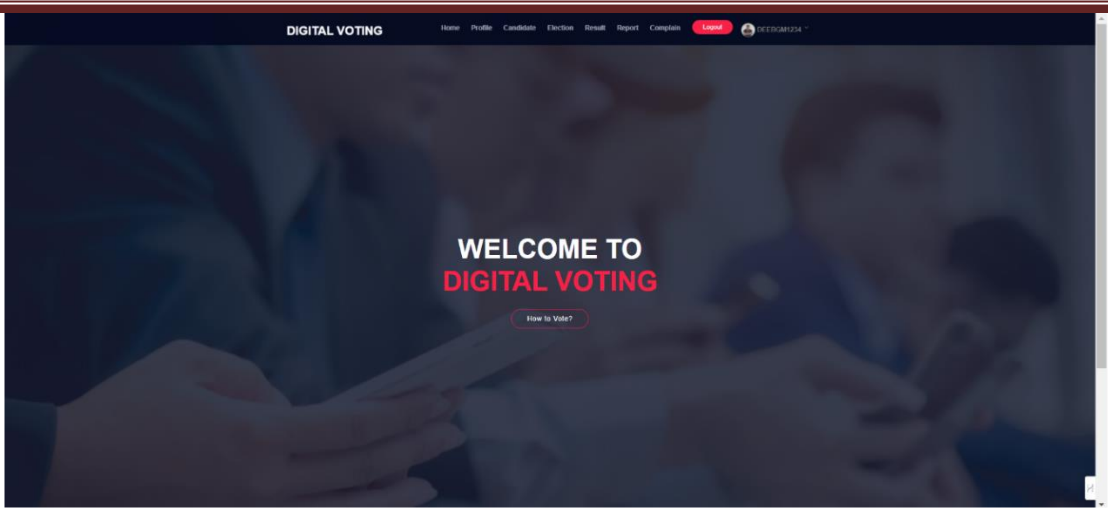

Figure 8.9 Voter Home page

The Voter Home page serves as the central hub for voters, offering access to essential features like vote casting, candidate information, and election updates within the voting system.

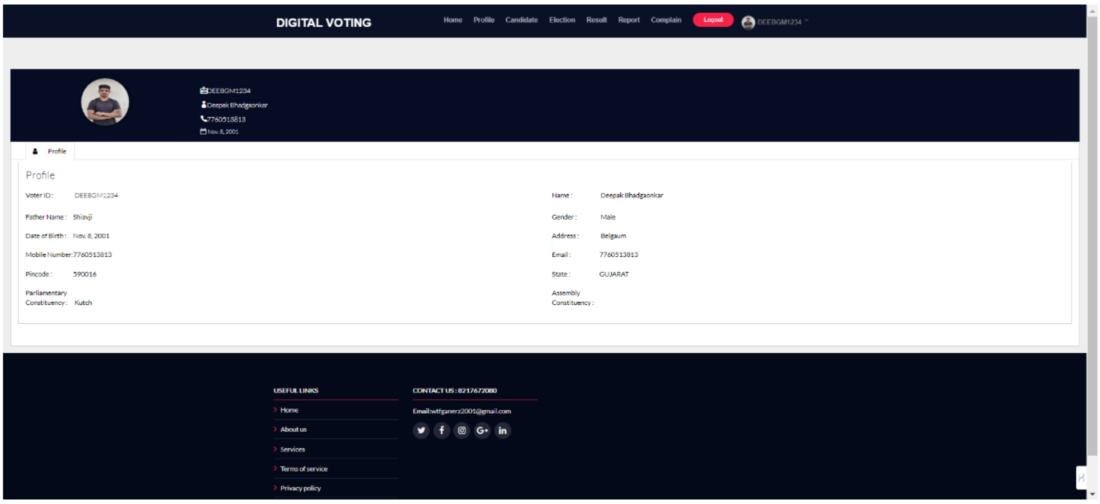

Figure 8.10 Profile

In profile section the voter can check their details and to which consistency they belong.

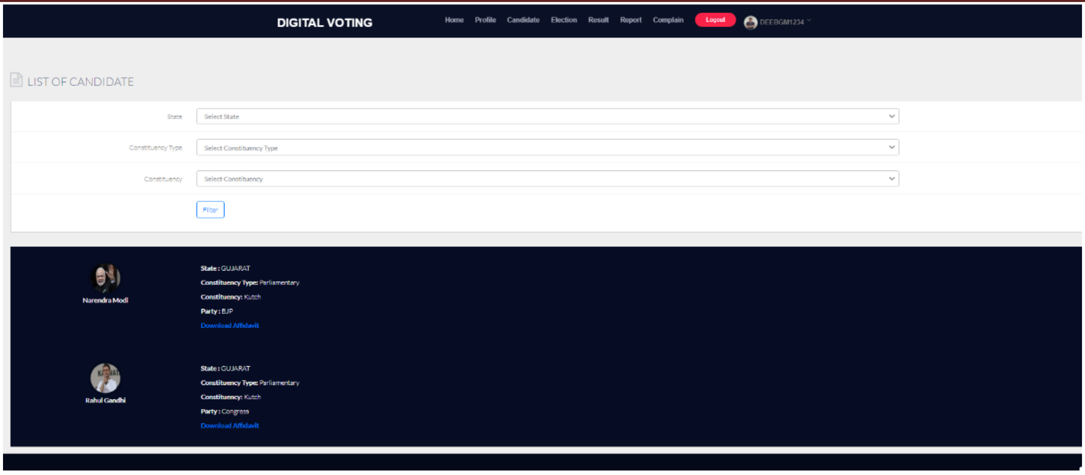

Figure 8.11 View Candidates

The "View Candidates" page enables users to browse and familiarize themselves with the candidates participating in the election, promoting informed voting decisions within the voting system.

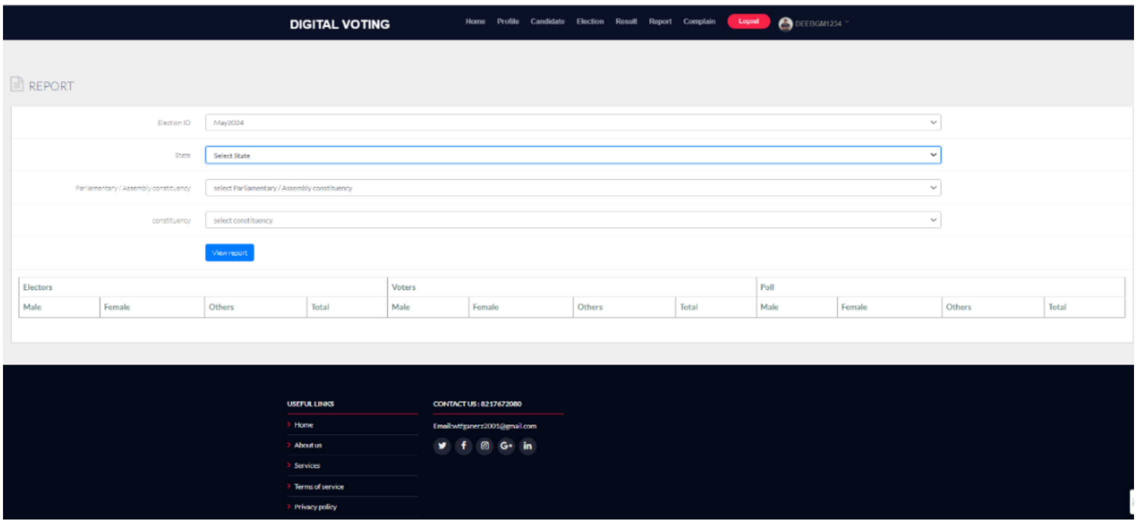

Figure 8.12 View election report

The "View Election Report" feature provides users with access to comprehensive reports detailing election results, ensuring transparency and accountability within the voting system.

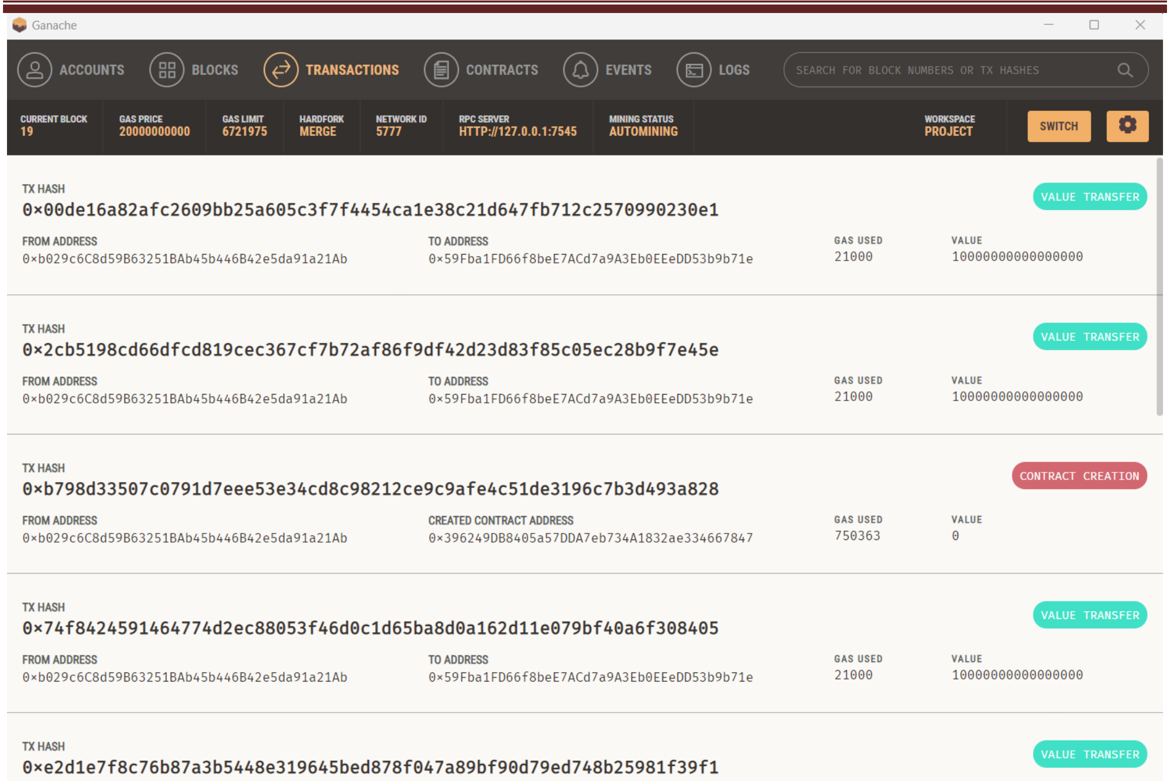

Figure 8.13 Ganache Transaction

In Ganache, a transaction begins with creation, where a user defines its parameters like recipient and amount, followed by signing using the sender's private key to ensure authenticity. The transaction is then broadcasted locally, immediately included in the next block, and confirmed almost instantly due to its local environment. If involving smart contracts, the transaction triggers state transitions within those contracts, potentially emitting events for further processing. Ganache offers a fast and efficient environment for testing Ethereum transactions and smart contract interactions, aiding developers in debugging and refining their decentralized applications without the constraints of the main Ethereum network.

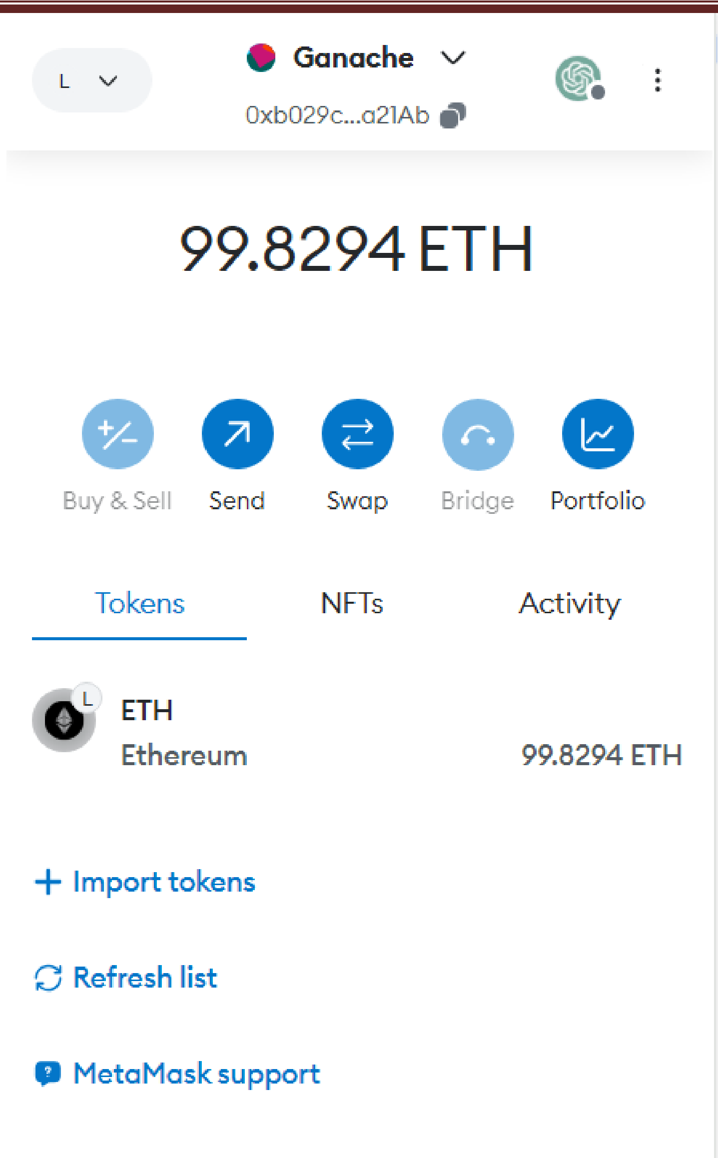

Figure 8.14 Metamask Wallet

Metamask is a cryptocurrency wallet and browser extension that enables users to interact with Ethereum-based decentralized applications (DApps) directly from their web browser. It allows users to securely store, send, and receive Ethereum and ERC-20 tokens, as well as access various Ethereum-based services and DApps seamlessly. With its intuitive interface and robust security features, Metamask simplifies the process of managing Ethereum assets and engaging with the decentralized web, making it an essential tool for both experienced cryptocurrency enthusiasts and newcomers to the space.

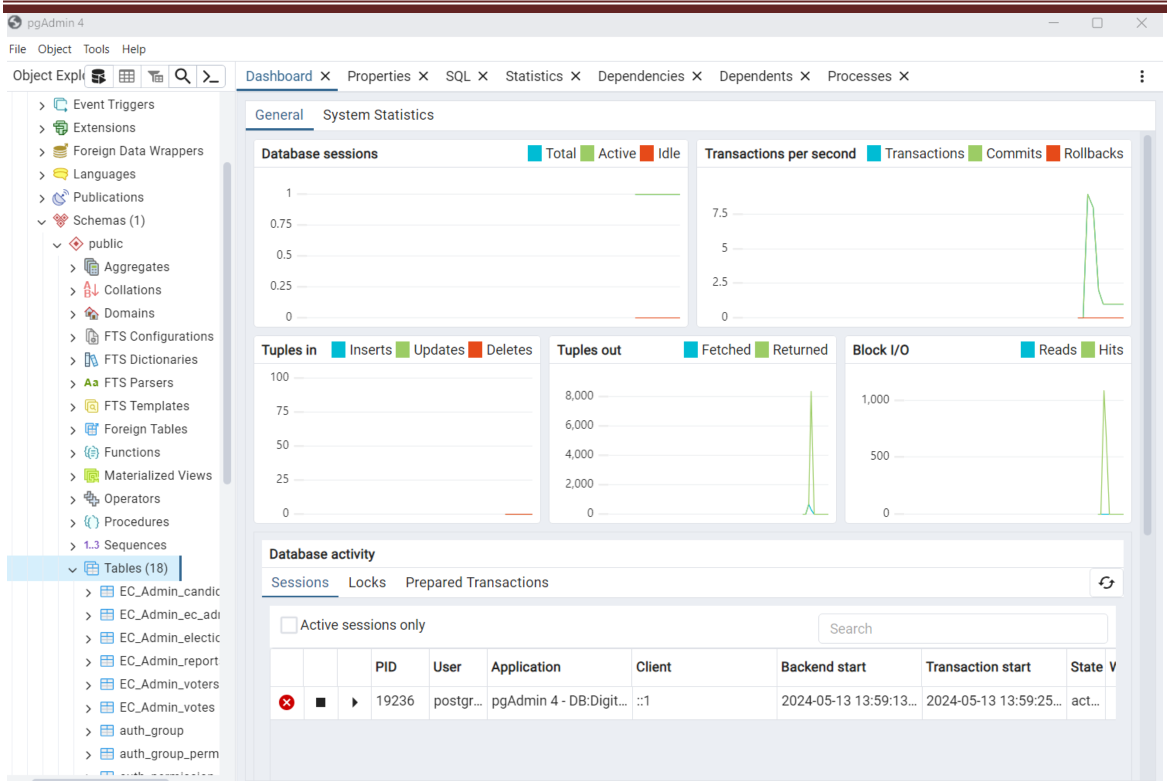

Figure 8.15 Database Transaction

In PostgreSQL, a database transaction represents a unit of work performed on the database that must be executed reliably and atomically. Transactions typically begin with the execution of one or more SQL statements, which can include data retrieval, manipulation, or schema modification. Once initiated, the transaction can either be committed, making its changes permanent and visible to other transactions, or rolled back, reverting any modifications made within the transaction to maintain the database's consistency and integrity. PostgreSQL ensures transactional reliability through features like ACID (Atomicity, Consistency, Isolation, Durability) properties, providing developers with a robust framework for managing concurrent access and ensuring data integrity within their applications.

CONCLUSION AND FUTURE SCOPE

CONCLUSION:

The execution of the blockchain-based e-voting system with face-recognition and OTP authentication represents a significant advancement in the realm of secure and transparent electoral processes. Through rigorous testing and validation, we have demonstrated the effectiveness and reliability of the system in ensuring the integrity of the voting process while preserving voter privacy. The integration of facial recognition technology and OTP authentication enhances the security of user authentication, mitigating the risk of unauthorized access and ensuring that only eligible voters can participate in the electoral process. The utilization of blockchain technology provides a secure and tamper-resistant platform for recording and verifying votes, promoting transparency and trust in the electoral outcome. Furthermore, the system's notification mechanism allows voters to receive immediate confirmation of their vote's successful recording without compromising their anonymity or revealing their voting preferences. This ensures that voters can have confidence in the integrity of the electoral process while maintaining their privacy.

In conclusion, the blockchain-based e-voting system with face-recognition and OTP authentication represents a robust and innovative solution to modernize and safeguard the democratic process, paving the way for more transparent and inclusive elections.

FUTURE SCOPE:

Scalability: Implementing sharding or layer 2 scaling solutions to accommodate increasing voter numbers and transaction volumes.

Usability: Enhancing user interfaces and integrating biometric authentication for user-friendly experiences.

Privacy: Employing zero-knowledge proofs or secure multiparty computation to protect voter privacy while ensuring result transparency.

Regulatory Compliance: Collaborating with authorities to establish regulatory frameworks that balance election integrity with blockchain innovation.

REFERENCES

[1]. Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K.-K.-R. (2022). The application of the blockchain technology in voting systems: A review. ACM Computer Survey, 54(3), 1–28.

[2]. Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: From internet voting to blockchain voting. J. Cybersecurity, 7(1), 1–15.

[3]. Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the design and implementation of a blockchain enabled E-Voting application within IoT oriented smart cities. IEEE Access, 9, 34165–34176.

[4]. Dimitriou, T. (2020). Efficient, coercion-free and universally verifiable blockchain based voting. Computer Network, 174, Art. no. 107234.

[5]. Farooq, M. S., Khan, M., & Abid, A. (2020). A framework to make charity collection transparent and auditable using blockchain technology. Comput. Electr. Eng., 83, Art. no. 106588.

[6]. Barnes, C., Brake, C., & Perry, T. (2022). Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers-Plymouth University. Accessed: Feb. 14.

[7]. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A., & Vora, P. (2008). E-voting scan integrity: End-to-end voter verifiable optical-scan voting. IEEE Security. Privacy, 6(3), 40–46.

[8]. Kim, T., Ochoa, J., Faika, T., Mantooth, A., Di, J., Li, Q., & Lee, Y. (2020). An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron.

[9]. Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. Technol. Forecast. Soc. Chang., 158, 120166.

[10]. Ometov, A., Bardinova, Y., Afanasyeva, A., Masek, P., Zhidanov, K., Vanurin, S., Sayfullin, M., Shubina, V., Komarov, M., & Bezzateev, S. (2020). An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future Trends. IEEE Access, 8, 103994–104015.

[11]. Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Netw., 34, 8–1

[12]. Çabuk, U. C., Adiguzel, E., & Karaarslan, E. (2020). A survey on feasibility and suitability of blockchain techniques for the e-voting systems. arXiv, arXiv:2002.07175.

[13]. Zhu, W., Tan, H., Zhao, J., Da Xu, L., & Guo, K. (2021). A novel service level agreement model using blockchain and smart contract for cloud manufacturing in industry 4.0. Enterp. Inf.Syst.

[14]. Shukur, I., Bakar, Z., & Bakar, K. A. A. (2020). A Study on Public Blockchain Consensus Algorithms: A Systematic Literature Review. Preprints.

[15]. Chan, S., Chu, J., Zhang, Y., & Nadarajah, S. (2020). Blockchain and Cryptocurrencies. J. Risk Financ. Manag., 13, 227.

APPENDIX-B

1.List of Events Attended Within State

SL.NO	Type of Event	Date	Place
1	National Level Project Competition	13/04/2024	Bangalore