**A**

**Project Report**

on

# Online Voting System

submitted for partial fulfillment for the award of

# BACHELOR OF TECHNOLOGY

# DEGREE

in

## Computer Science

By

Ashish Kumar Gupta (2000290120043)

Aditya Aggarwal (2000290120013)

Saurabh Pundir (2000290110149)

**Under the Supervision of**

Mr. Akash Goel

Assistant Professor

## Department of Computer Science

## KIET Group of Institutions, Ghaziabad

Affiliated to

## Dr. A.P.J. Abdul Kalam Technical University, Lucknow

# DECLARATION

We hereby declare that this submission is our own work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Ashish Kumar Gupta (2000290120043)
Aditya Aggarwal (2000290120013)
Saurabh Pundir (2000290110149)
Date:-


# CERTIFICATE

This is to certify that Project Report entitled "Online Voting System" which is submitted by in partial fulfillment of the requirement for the award of degree B. Tech. in Department of Computer Science of Dr. A.P.J. Abdul Kalam Technical University, Lucknow is a record of the candidates own work carried out by them under my supervision. The matter embodied in this report is original and has not been submitted for the award of any other degree.

Date:

**Supervisor Signature**

Mr. Akash Goel
Assistant Professor
Department of
Computer Science

# ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the report of the B. Tech Project undertaken during B. Tech. Final Year. We owe special debt of gratitude to Assistant Professor Akash Goel Department of Computer Science, KIET, Ghaziabad, for his constant support and guidance throughout the course of our work. His sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only his cognizant efforts that our endeavors have seen light of the day.

We also take the opportunity to acknowledge the contribution of Dr. Ajay Kumar Shrivastava, Head of the Department of Computer Science, KIET, Ghaziabad, for his full support and assistance during the development of the project. We also do not like to miss the opportunity to acknowledge the contribution of all the faculty members of the department for their kind assistance and cooperation during the development of our project.

Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

Signature
Name:- Ashish Kumar Gupta
Roll No.:- 2000290120043

Signature
Name:- Aditya Aggarwal
Roll No.:- 2000290120013

Signature
Name:- Saurabh Pundir
Roll No.:- 2000290110149

# ABSTRACT

In our project, we address the challenge of building a secure online voting system that upholds the fairness and privacy of traditional voting methods while leveraging the transparency and flexibility offered by electronic systems. It focuses on the application of blockchain technology to develop a distributed online voting system. We propose an innovative blockchain-based voting system designed to overcome the limitations of existing online voting platforms. Our project involves evaluating various popular blockchain frameworks to determine their effectiveness in constructing a robust online voting solution. Through a detailed case study of an election process, we demonstrate how our blockchain-based application can enhance security and reduce the costs associated with conducting nationwide elections. Our system employs cryptographic techniques to ensure that votes are tamper-proof and verifiable, addressing major concerns of voter fraud and manipulation. Additionally, the decentralized nature of blockchain helps prevent single points of failure, ensuring system reliability and uptime. By utilizing blockchain technology, our project aims to increase voter confidence by ensuring that their votes are secure, transparent, and accurately counted. Furthermore, the system is designed to be user-friendly, making it accessible to a broad demographic of voters, thereby encouraging higher voter turnout. Our approach not only promises to revolutionize the way elections are conducted but also sets a new standard for trust and efficiency in online voting systems.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| DFD | Data Flow Diagram |
| ER | Entity Relationship |
| IPFS | InterPlanetary File System |
| ROI | Return on investment |
| IEEE | Institute of Electrical and Electronics Engineers |
| SWOT | Strengths, Weaknesses, Opportunities, and Threats |
| PEST | Political, Economic, Social and Technological factors |
| MVP | Minimum Viable Product |
| UAT | User Acceptance Testing |
| API | Application Programming Interface |
| IDE | Integrated Development Environment |
| UI | User Interface |
| ECC | Error correction code memory |

# CHAPTER 1
# INTRODUCTION

## 1.1 Introduction to Project

In this project, our aim is to create a cutting-edge electronic voting system leveraging blockchain technology. This system will revolutionize the voting process by allowing individuals to cast their votes conveniently from anywhere using electronic devices like mobile phones or computers. Despite the potential benefits, widespread adoption of such systems has been hindered by legitimate security concerns. Issues such as hacking and manipulation pose significant threats to the integrity of elections, prompting caution in their implementation on a larger scale. However, by incorporating blockchain's decentralized and secure nature, we endeavor to address these concerns and pave the way for a more transparent and trustworthy voting process.

**Benefits of blockchain based e-voting system to customers.**

**Fairness and Privacy**: With blockchain technology, votes are encrypted and stored securely, ensuring that each vote remains anonymous and tamper-proof. This ensures the integrity of the voting process and maintains the privacy of voters, fostering trust in the system.

**Speed and Efficiency**: Electronic voting via blockchain eliminates the need for manual counting and reduces the time required to tally votes. This results in a faster and more efficient voting process, enabling quicker declaration of results and reducing the likelihood of errors.

**Transparency**: The decentralized nature of blockchain ensures that every transaction (in this case, votes) is recorded transparently and cannot be altered retroactively. This transparency builds trust among voters, as they can independently verify the integrity of the voting process.

**Immutability**: Once a vote is recorded on the blockchain, it becomes immutable, meaning it cannot be changed or deleted. This feature ensures the integrity of the voting data and prevents any unauthorized alterations, thus enhancing the reliability of the electoral outcome.

## 1.2 Project Category

The development of an online voting system using blockchain technology is a pivotal endeavor in modernizing the electoral process, aiming to establish a trustworthy, inclusive, and efficient platform for democratic participation. This ambitious project involves crafting a

user-friendly web application or system that empowers voters to cast their ballots remotely via electronic devices like computers, smartphones, or tablets. By harnessing the power of blockchain technology, the integrity and immutability of the voting process are upheld, with each vote securely encrypted, recorded, and stored on a decentralized ledger. Moreover, the system may incorporate advanced features such as identity verification, fraud prevention, and real-time result monitoring to further enhance transparency and security. Meticulous attention is dedicated to ensuring reliability, security, and usability across various stages, including requirements analysis, system design, software development, testing, and deployment, thereby advancing the integrity and accessibility of democratic elections in the digital era.

## 1.3 Objectives

Our objective is to develop a Digital Voting System with several key functionalities to ensure the integrity, accessibility, and trustworthiness of the electoral process. Firstly, the system will authenticate voters' identities to ensure that only registered individuals are eligible to cast their ballots, thereby preventing unauthorized access and maintaining the integrity of the voting process. Additionally, stringent measures will be implemented to ensure that each registered voter can only vote once, preventing instances of double voting or voter fraud. Furthermore, the system will securely store each voter's individual vote, safeguarding the confidentiality and privacy of their choices while also enabling accurate auditing and verification of the voting results.

Secondly, the user interface of the Digital Voting System will be intuitively designed to facilitate easy and seamless voting for all eligible individuals. This includes providing accessibility features to accommodate voters with diverse needs and ensuring compatibility with a wide range of electronic devices such as smartphones, tablets, and computers. Moreover, efforts will be made to promote widespread participation by eliminating barriers to entry and ensuring that every eligible voter, regardless of location or circumstance, can exercise their democratic right to vote.

Lastly, paramount importance will be given to the transparency and trustworthiness of the vote tallying process. Through the utilization of robust cryptographic techniques and blockchain technology, the Digital Voting System will ensure the verifiability and immutability of the voting results, thereby instilling confidence in the accuracy and fairness of the electoral

outcomes. By providing a secure, accessible, and transparent voting platform, our objective is to enhance democratic governance and foster public trust in the electoral process.

## 1.4 Structure of Report

**CHAPTER 1: INTRODUCTION**

1.1 Introduction to Project: Provide an overview of the project, its purpose, and relevance.

1.2 Project Category: Define the category or domain the project belongs to.

1.3 Objectives: List the specific goals and objectives of the project.

1.4 Structure of Report: Outline the structure and organization of the report.

**CHAPTER 2: LITERATURE REVIEW**

2.1 Literature Review: Summarize existing research and literature relevant to the project.

2.2 Research Gaps: Identify gaps or areas where further research is needed.

2.3 Problem Formulation: Clearly state the problem or issue the project aims to address.

**CHAPTER 3: PROPOSED SYSTEM**

3.1 Proposed System: Describe the proposed solution or system to address the identified problem.

3.2 Unique Features of The System: Highlight the distinctive features or innovations of the proposed system.

**CHAPTER 4: REQUIREMENT ANALYSIS AND SYSTEM SPECIFICATION**

4.1 Feasibility Study: Assess the feasibility of the proposed system in terms of technical, economic, and operational aspects.

4.2 Software Requirement Specification: Detail the specific requirements of the software system.

4.3 SDLC Model Used: Specify the software development life cycle model used for the project.

4.4 System Design: Present the overall design of the system, including data flow diagrams, use case diagrams, and database design.

**CHAPTER 5: IMPLEMENTATION**

5.1 Introduction Tools and Technologies Used: Introduce the tools, technologies, and methodologies used in the implementation of the project.

**CHAPTER 6: TESTING AND MAINTENANCE**

6.1 Testing Techniques and Test Cases Used: Describe the testing methods employed and present test cases used to validate the system.

6.2 Maintenance: Discuss plans for system maintenance and future updates.

**CHAPTER 7: RESULTS AND DISCUSSIONS**

7.1 Description of Modules with Snapshots: Provide an overview of system modules and include screenshots or snapshots.

7.2 Key findings of the project: Summarize the main results and outcomes of the project.

7.3 Brief Description of Database with Snapshots: Describe the database structure and include relevant snapshots.

**CHAPTER 8: CONCLUSION AND FUTURE SCOPE**

Conclusion: Summarize the main findings and outcomes of the project.

Future Scope: Discuss potential future enhancements, extensions, or research directions related to the project.

# CHAPTER 2

# LITERATURE REVIEW

## 2.1 Literature Review

**Table no. 2.1**

**Literature Review**

| Sr. No | Title of the Paper with Author(s) Name | Journal/ Conference | Year | Highlights |
|---|---|---|---|---|
| 1 | Blockchain And The Future of the Internet: A Comprehensive Review by Fakhar ul Hassan, Anwaar Ali, Siddique Latif, Junaid Qadir, Salil Kanhere, Jatinder Singh, and Jon Crowcroft | Journal | 2019 | In this research Jon Crowcroft, emphasizes blockchain's role in challenging the centralized trust infrastructure of the internet. It highlights its principles of decentralization and transparency, showcasing its applications in diverse fields. The paper surveys blockchain-based network applications and provides guidance while addressing potential challenges, making it a reference manual for interested parties. |
| 2 | User-Perceived Privacy in Blockchain by Simin Ghesmati, Walid Fdhila, and Edgar Weippl | Journal | 2022 | In this research by Simin Ghesmati, Walid Fdhila, and Edgar Weippl, users privacy perceptions in UTXO-based blockchains like Bitcoin are investigated. The research, which involves interviews and questionnaires, aims to establish a mental model for employing |

| | | | | |
|---|---|---|---|---|
| | | | | privacy-preserving techniques in blockchain transactions. Additionally, it evaluates users awareness of blockchain privacy issues and their preferences regarding existing privacy enhancing solutions, comparing add-on techniques for Bitcoin to builtin techniques in privacy coins. The research uses Bitcoin as an example to highlight discrepancies between user privacy perceptions, preferences, and current implementations. |
| 3 | Blockchain Technology and its Impact on the Global Economy by Dr. Burcu Sakız (Istanbul Aydın University, Turkey) Prof. Dr. Aysen Hic Gencer (Beykent University, Turkey) | Conference | 2019 | In this research Dr. Burcu Sakız and Prof. Dr. Ayşen Hiç's explores the economic landscape of blockchain technology. Data has become the most valuable resource in today's world, surpassing oil. With smartphones and the internet, data has become abundant and invaluable. Modern algorithms and AI extract predictive insights. Blockchain is presented as a decentralized, fair-sharing mechanism for knowledge. It enables secure, direct transactions without intermediaries, disrupting traditional finance and enhancing economic transparency. |
| 4 | Blockchain Research, | Journal | 2019 | In this research Laurie Hughes, |

| | | | | |
|---|---|---|---|---|
| | Practice and Policy: Applications, Benefits, Limitations, Emerging Research Themes and Research Agenda by Laurie Hughes, Yogesh K. Dwivedi, Santosh K Misra, Nriprenda Rana | | | Yogesh K. Dwivedi, Santosh K Misra, Nriprenda Rana analyzed that the blockchain has gained substantial attention in technology research, but its adoption in Information Systems (IS) and Information Management (IM) literature has been slow. This study, through an IS/IM perspective, reviews existing blockchain research to identify key themes. Although commercial-grade blockchain applications are currently limited, the technology shows significant potential for various industry-wide use cases. The research discusses potential blockchain applications, the technology's future, and the barriers to adoption. It also highlights the blockchain's potential to contribute to UN Sustainability Development Goals and drive change in established industries and practices. |
| 5 | Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto | Journal | 2009 | In this research by Satoshi Nakamoto, the concept of a purely peer-to-peer electronic cash system is introduced. It enables online payments to occur directly between parties without the need for intermediaries. To address the issue of double spending, the research |

| | | | | |
|---|---|---|---|---|
| | | | | proposes a peer-to-peer network that timestamps transactions through proof-of-work, creating an immutable transaction record. The longest proofof-work chain, backed by the majority of CPU power, serves as proof of the transaction history's authenticity, making the network resilient to attacks and adaptable to node dynamics. Messages are distributed with minimal structure, allowing nodes to join and leave the network as needed. |
| 6 | Blockchain technology in the energy sector: A systematic review of challenges and opportunities by Merlinda Andoni, Valentin Robu, David Flynn, Simone Abram | Journal | 2019 | Blockchain technology has rapidly gained attention and comparison with other technologies, particularly regarding energy consumption and environmental impact. This study by Merlinda Andoni, Valentin Robu, David Flynn, and Simone Abram reviews 140 blockchain research 8 projects and startups to create a map of blockchain's potential in energy applications. It categorizes these initiatives by field and implementation platform and discusses various use cases, including P2P energy trading and IoT applications. The paper also addresses challenges and market barriers for blockchain's |

| | | | | |
|---|---|---|---|---|
| | | | | mainstream adoption in the energy sector. |
| 7 | Machine Translation using Semantic Web Technologies: A Survey by Diego Moussallem, Matthias Wauer, Axel-Cyrille Ngonga Ngomo | Journal | 2017 | In this research Diego stated that many machine translation approaches have recently been developed to facilitate the fluid migration of content across languages. However, the literature suggests that many obstacles must still be dealt to achieve better automatic translations. |
| 8 | An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends by Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping | Conference | 2010 | In this research by Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping. Blockchain is gaining attention for its decentralized, immutable ledger for transactions. It's applied in finance, reputation systems, IoT, and more. This paper offers an overview of blockchain architecture, compares algorithms used, highlights challenges like scalability and security, and discusses future trends in blockchain technology |
| 9 | How are Solidity smart contracts tested in open source projects? An exploratory study by Luisa Palechor, Cor-Paul Bezemer | Conference | 2022 | This study by Luisa Palechor and Cor-Paul Bezemer examines the testing of smart contracts in 139 open-source Solidity projects on the blockchain. It reveals that core developers typically handle contract testing, with functional testing frameworks, particularly Truffle, |

| | | | | |
|---|---|---|---|---|
| | | | | being commonly used. Functional testing is widespread (93%), while security testing is less common (9.4%), and traditional performance testing is absent. Additionally, 34 projects mentioned external audit reports. |
| 10 | Ethereum and Its Future: A Review of Cryptocurrency by Pavan Kumar S, Lalit Kumar, Prajwal B.I, Pranav Sabarinath Nair, Anjali K, and Vrinda U | Journal | 2022 | In this research by 9 Pavan Kumar S, Lalit Kumar, Prajwal B.I, Pranav Sabarinath Nair, Anjali K, and Vrinda U. Ethereum's use, and applications are on the rise, driving an increased interest in cryptocurrencies. However, with technological advancements, security threats also grow. It is crucial to safeguard privacy and data. While blockchain, known for Bitcoin, offers security, it extends to various other currencies and tokens. Exploring Ethereum reveals its uses, vulnerabilities, and protective applications for the future. |

## 2.2 Research Gaps

**Table no. 2.2**

**Research Gaps**

| References | Research Gaps |
|---|---|
| [1] Blockchain And The Future of the Internet: A Comprehensive Review | Need for further empirical research to evaluate the effectiveness and scalability of these applications in real-world scenarios. |
| [2] User-Perceived Privacy in Blockchain | Need for understanding the underlying factors influencing discrepancies between users privacy perceptions and preferences and current implementations. |
| [3] Blockchain Technology and its Impact on the Global Economy | It falls short in providing a comprehensive analysis of the challenges and limitations that may impede its widespread adoption and impact. |
| [4] Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda | There remains a notable gap in the Information Systems (IS) and Information Management (IM) literature regarding the comprehensive exploration and integration of blockchain applications. |
| [5] Bitcoin: A Peer-to Peer Electronic Cash System | There may be challenges or limitations in terms of scalability, security, or efficiency that warrant further exploration. |
| [6] Blockchain technology in the energy sector: A systematic review of challenges and opportunities | A notable research gap exists in the area of assessing the long-term sustainability and scalability of these initiatives, it lacks in-depth analysis regarding the real-world implementation challenges, regulatory hurdles, and potential environmental impacts associated with scaling these solutions. |
| [7] Machine Translation Using Semantic Web Technologies: A Survey | There remains a notable gap in understanding the effective integration and optimization of these technologies within existing translation systems. Further investigation is warranted to explore strategies for leveraging semantic web technologies |

| | |
|---|---|
| | to address the issue of ambiguity and improve the overall efficacy of machine translation systems. |
| [8] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends | While the paper offers a thorough examination of blockchain technology, encompassing its architecture, consensus algorithms, technical challenges, advances, and future trends, there appears to be a gap in the explicit exploration of solutions to scalability and security issues within blockchain systems. |
| [9] An Exploratory Study of Smart Contracts in the Ethereum Blockchain Platform | There remains a gap in understanding the evolution of smart contracts and their usage patterns beyond this timeframe. |

## 2.3 Problem Formulation

The traditional methods of conducting elections are often plagued by inefficiencies, vulnerabilities, and lack of transparency, leading to challenges such as voter fraud, tampering of results, and logistical constraints. In light of these issues, there is a pressing need for the development of a secure, transparent, and accessible voting system that leverages blockchain technology to ensure the integrity and fairness of the electoral process. The absence of a robust online voting solution leaves a void in democratic governance, hindering the ability to conduct elections efficiently, accurately, and inclusively. Therefore, the primary objective of this project is to design and implement an Online Voting System using blockchain technology, addressing the aforementioned challenges and providing a reliable platform for citizens to exercise their democratic rights with confidence and trust.

# CHAPTER 3

# PROPOSED SYSTEM

## 3.1 Proposed System

### 3.1.1 ARCHITECTURE

The envisioned architecture for the e-voting system has been structured into multiple layers, aiming for a modular design approach. These distinct layers are elaborated upon as follows:

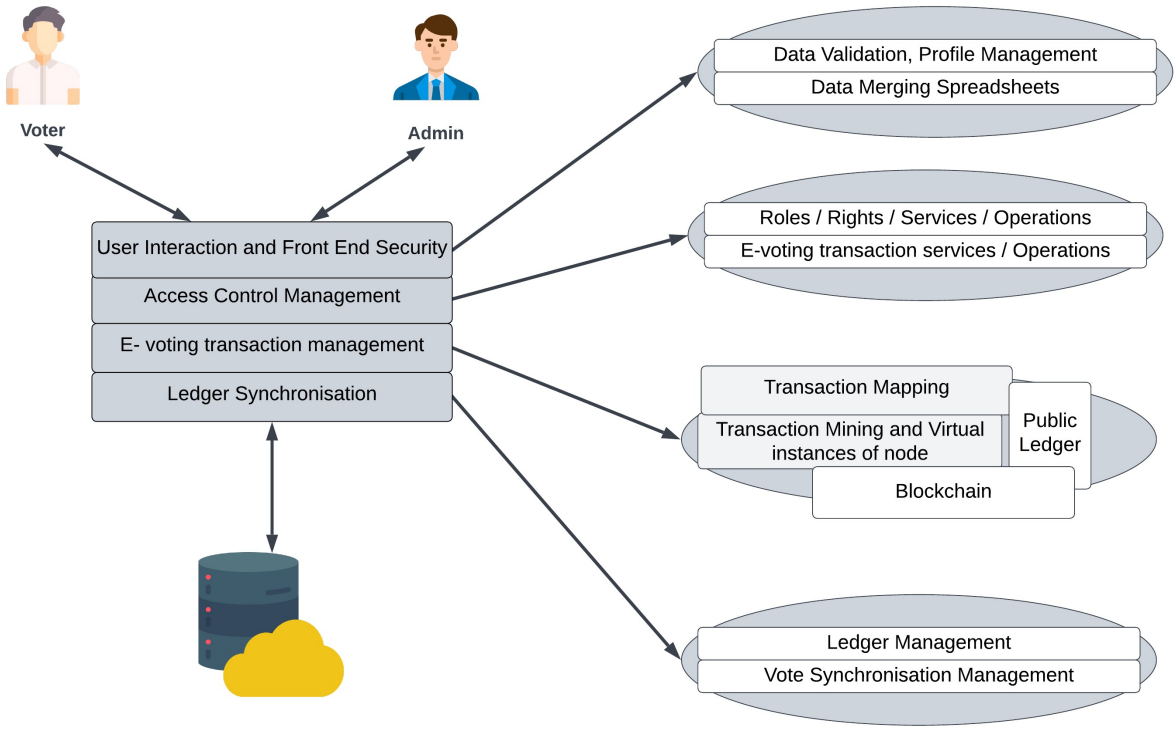



**Fig 3.1**

**Architecture**

#### 3.1.1.1 User Interaction and Front-End Security

The User Interaction and Front-end Security layer manages interactions with both voters (enabling vote casting) and administrators (overseeing the election process). Its core functions revolve around authenticating and authorizing users—ensuring that system access remains exclusive to authorized individuals as per predefined access control policies. This layer employs diverse authentication methods, ranging from conventional username/password

setups to sophisticated techniques like fingerprinting or iris recognition, tailored to suit the architecture's specifics. Essentially, it serves as the primary interface for users, responsible for validating user credentials based on systemspecific policies.

#### 3.1.1.2 Access Control Management Layer

The Access Control Management layer serves as a foundational support system for both Layer 1 and Layer 3, providing essential services crucial for these layers to fulfill their respective objectives. Its services encompass role definition, establishing associated access control policies, and outlining specifications for voting transactions. Role definition and management form the core of access control operations in Layer 1, while voting transaction definitions aid in mapping blockchain-based transactions for processing in Layer 3. Essentially, this layer synchronizes the functionalities of the proposed system by providing fundamental elements necessary for each individual layer's operations.

#### 3.1.1.3 Transaction Management Layer

The E-Voting Transaction Management layer serves as the central core within the architecture. Here, the e-voting transaction constructed at the Role Management/Transactions layer is linked to the blockchain transaction for mining purposes. This linked transaction incorporates the voter's provided credentials from Layer 1, such as the voter's fingerprint, for authentication. This data is utilized to generate a cryptographic hash that contributes to forming the transaction ID. The verification of these credentials is intended to occur at the User Interaction and Front-end Security layer (Layer 1). The process involves several virtual node instances participating in mining to finalize the transaction's entry into the blockchain.

#### 3.1.1.4 Ledger Synchronization Layer

The Ledger Synchronization layer is responsible for harmonizing the Multichain ledger with a dedicated local application database, utilizing an established database technology. Votes cast are logged in the backend data tables of this database. Voters are furnished with a unique identifier upon the immediate addition of their vote into the blockchain ledger, enabling them to track their votes. The security of votes relies on blockchain technology, employing cryptographic hashes to ensure secure end-to-end communication. Additionally, voting results

are stored within the application's database, intending to ease auditing processes and enable further operations at subsequent stages.

### 3.1.2 ALGORITHM USED

Blockchains function based on consensus algorithms, which enable agreement among distributed nodes. These mechanisms are pivotal in fostering reliability, trust, and security within the network. Consensus methods like proof of work (PoW) or proof of stake (PoS) act as vital safeguards, preventing unauthorized validation of inaccurate transactions and bolstering network security. They are crucial for maintaining the confidentiality and integrity of shared information across the blockchain. Additionally, Elliptic Curve Cryptography (ECC) is utilized. ECC, as a form of asymmetric cryptography, relies on the mathematical principles of elliptic curves for encryption.

$$y^2 = x^3 + ax + b\text{……..}$$

**Working of ECC**

**Step1- Key Pair Generation**: - Within Elliptic Curve Cryptography (ECC), a user's private key is randomly generated, while the corresponding public key is generated using elliptic mathematics. Both the private and public keys are maintained in secrecy to ensure the security of the cryptographic system.

**Step2- Public Key Distribution**: - The public key is shared with the server or other person who wants to send encrypted data. The public key is safe to distribute widely.

**Step3- Encrypting the data**: - When the server or other person wants to send the data, the data is encrypted with the help of recipient's public key.

**Step4- Decryption**: - The recipient possesses a corresponding private key, utilized specifically for decrypting the data. The mathematical properties of elliptic curves guarantee the efficiency of the private key in executing this decryption process.

Consider a scenario where two individuals, referred to as Person 1 and Person 2, engage in communication and data exchange. Both parties share a mutual elliptic curve equation along with a generator point denoted as G.

Let private keys of ***Person 1*** and ***Person 2*** are $\boldsymbol{nA}$ and $\boldsymbol{nB}$ respectively. Now, public keys of both are given as,

$$K_1 = nAG$$

and

$$K_2 = nBG$$

If Person 1 intends to send a message M to Person 2, they utilize the public key of Person 2 to encrypt the message. The resulting ciphertext is computed as follows:

$$C = \{\lambda G, M + \lambda K2\}$$

where $\boldsymbol{\lambda}$ is any random number, which makes sure that for same message each time a different cipher text is generated. This will make it hard for someone who is trying to decrypt the message illegally.

Now for decryption process of message, person 2 can decrypt the message by subtracting the coordinate of $\lambda G$ multiplied by $nB$ from $M + \lambda K2$ . The decrypted message is given by,

$$M = \{M + \lambda K2 - nB\lambda G\}$$

(This multiplication is not simple algebraic multiplication, but it is multiple addition of points - geometrical).

### 3.1.3 IMPLEMENTATION

#### 3.1.3.1 Description of the implementation

Logging in to the web application with the help of unique address on which Smart contract is deployed. Only the deployed address has administration privileges.

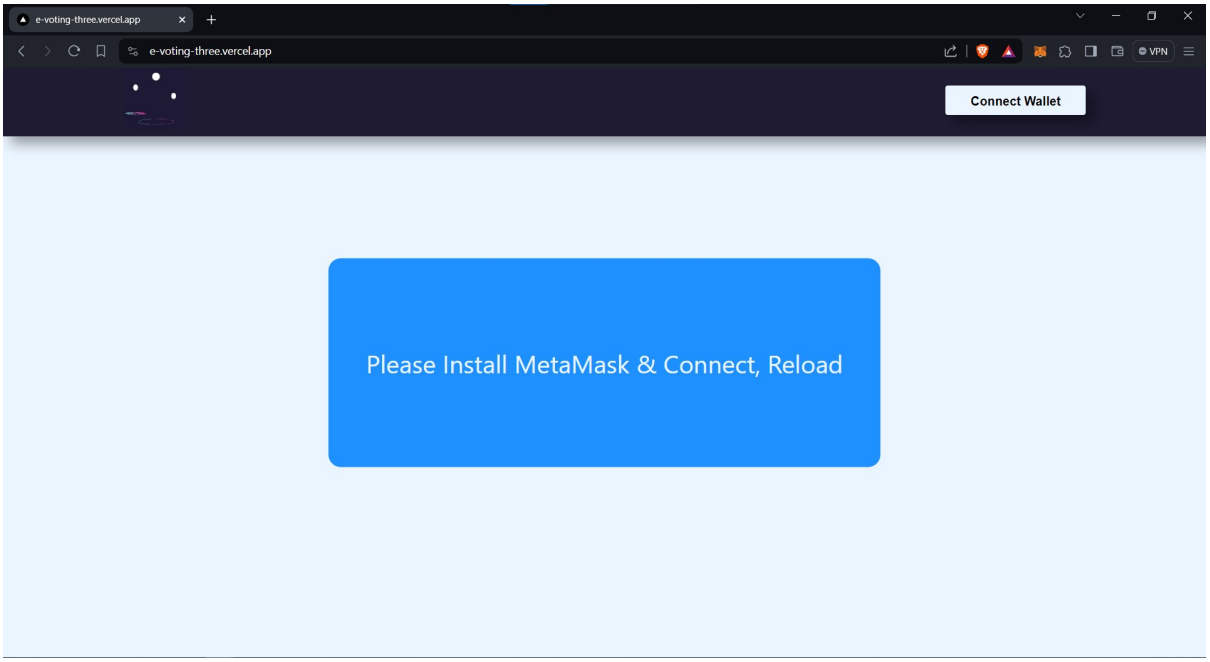



**Fig 3.2**

**Home page of e-voting system**

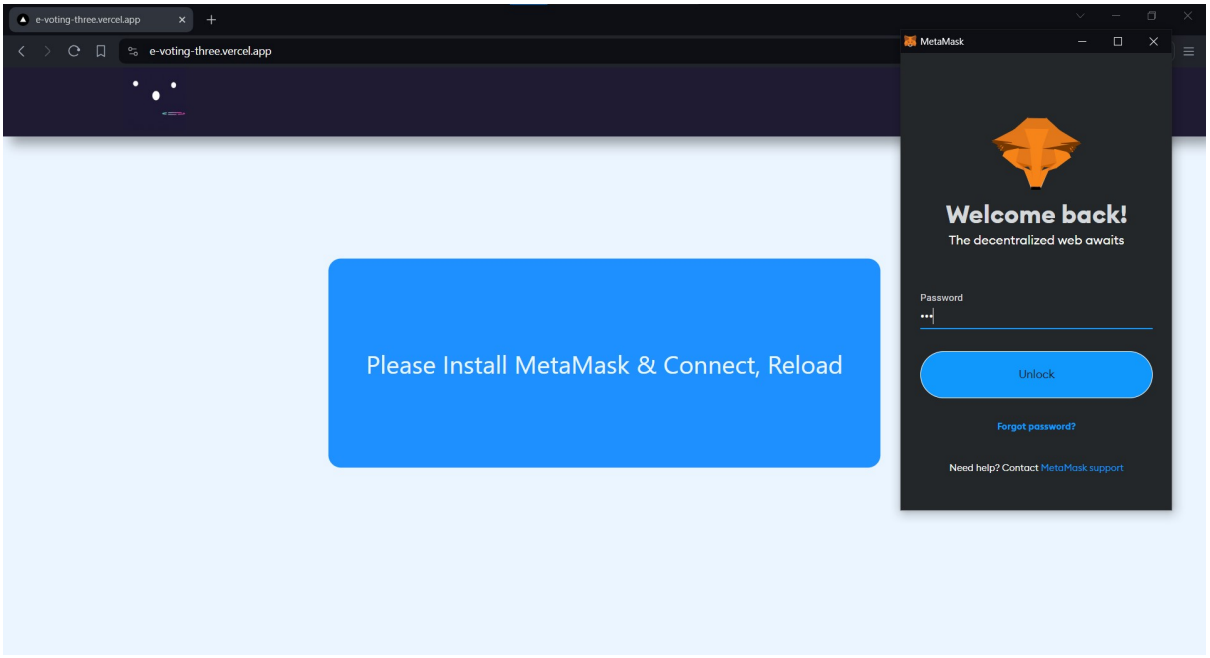



**Fig 3.3**

**Logging in to MetaMask**

### 3.1.3.2 Registering the candidate

Navigating to the candidate registration page and registering the candidate. Entering the candidate details with the unique address. Uploading the image to the IPFS using the upload image button. Entering name address and other details.

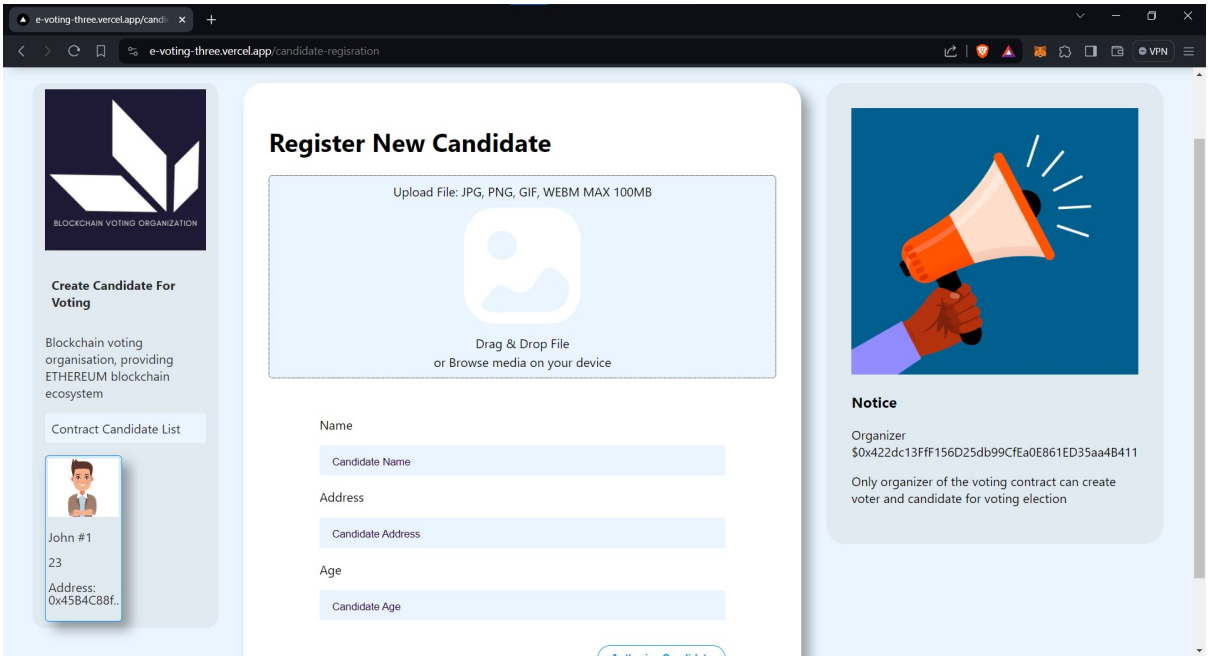



**Fig 3.4**

**Registering the Candidate**

### 3.1.3.3 Registering the Voter

Registering the voter same as the candidate registration.

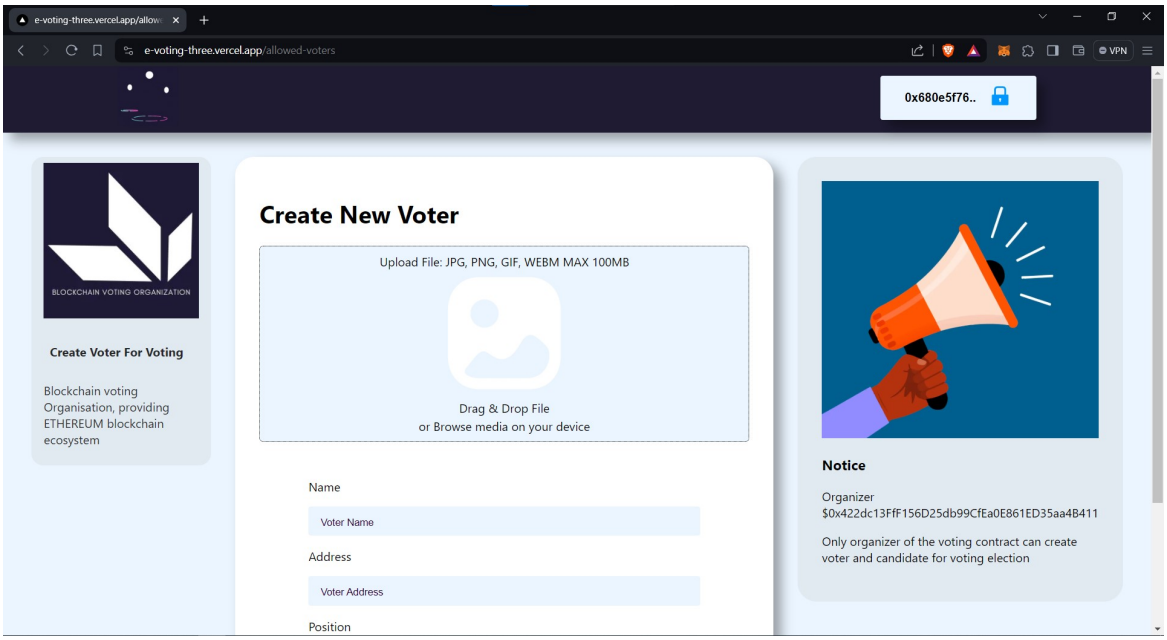



**Fig 3.5**

**Registering the Voter**

### 3.1.3.4 Voting process

Voter's logging to the application using registered account through MetaMask. After successful login the candidates are shown at the homepage itself. Voters vote by clicking the 'vote' button.

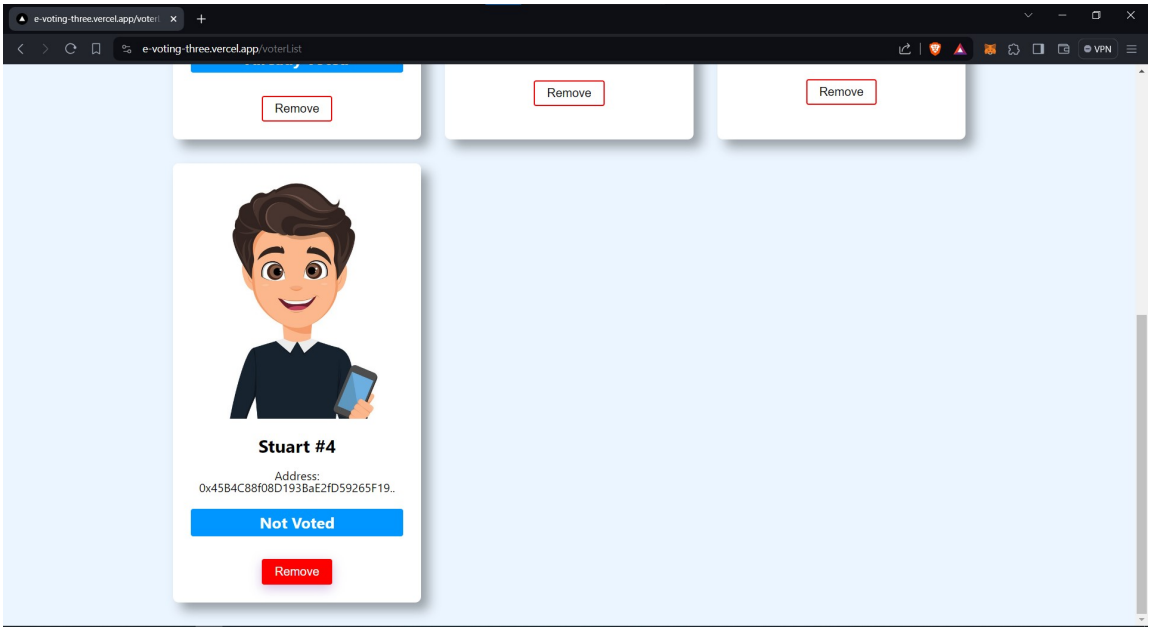



**Fig 3.6**

**Registered Candidates**

This is the whole mechanism of the voting process done by the proposed E-voting system where administrators can register and remove candidates and voters. Voters can vote to their choice of Candidates. As the whole process is done in the form of transaction on Ethereum blockchain it makes it more reliable.

## 3.2 Unique Features of The System

**Blockchain Integration:** The system will leverage blockchain technology to provide an immutable and transparent ledger for recording and storing voting transactions. This ensures that each vote is securely encrypted and timestamped, preventing tampering or manipulation of election results.

**Decentralized Verification:** Through the decentralized nature of blockchain, the voting process will be verified by a distributed network of nodes, eliminating the reliance on a central authority and enhancing the system's resilience against cyber attacks and fraud.

**Voter Anonymity:** While ensuring authentication and security, the system will maintain the anonymity of voters, protecting their privacy and confidentiality throughout the voting process.

**Voter Education and Engagement:** The project will include initiatives to educate voters about the benefits and procedures of online voting, fostering greater participation and trust in the electoral process among citizens of all demographics.

**Immutable Voter Records:** Utilizing blockchain technology, the system will maintain immutable records of voter registration, ensuring that once registered, a voter's information cannot be altered or tampered with, thereby enhancing the integrity of the voter database.

# CHAPTER 4

# SYSTEM REQUIREMENT ANALYSIS AND SYSTEM SPECIFICATION

## 4.1 Feasibility Study

### 4.1.1 Introduction:

Online voting systems have the potential to revolutionize democratic processes by making voting more accessible, secure, and transparent. Leveraging blockchain technology can address many of the challenges associated with traditional voting systems, such as fraud, tampering, and logistical issues. This feasibility study examines the technical, economical, and operational aspects of implementing an online voting system using blockchain technology.

### 4.1.2 Technical Feasibility:

**a. Blockchain Infrastructure:** Assess the scalability of blockchain technology to handle large-scale voting operations. Evaluate different blockchain platforms (e.g., Ethereum, Hyperledger) for suitability in terms of transaction throughput, consensus mechanisms, and smart contract capabilities. Determine the level of decentralization required to ensure security and integrity of the voting process.

**b. Security Measures:** Implement cryptographic techniques to ensure the anonymity and confidentiality of votes. Design robust authentication mechanisms to prevent unauthorized access and ensure voter eligibility. Evaluate methods for preventing double voting and ensuring the integrity of the voting process.

**c. User Experience:** Develop user-friendly interfaces for both voters and election administrators. Test the system for usability and accessibility across different devices and platforms. Incorporate features such as voter verification, ballot preview, and receipt generation to enhance transparency and trust in the system.

### 4.1.3 Economical Feasibility:

**a. Cost Analysis:** Estimate the initial investment required for developing the online voting system, including software development, infrastructure setup, and security measures. Assess ongoing operational costs, including maintenance, hosting, and support services. Compare the

costs of the proposed online voting system with traditional voting methods to determine cost-effectiveness.

**b. Return on Investment (ROI):** Evaluate the potential savings achieved through increased efficiency, reduced administrative overhead, and lower printing and distribution costs. Consider the long-term benefits of improved voter participation, enhanced transparency, and trust in the electoral process.

### 4.1.4 Operational Feasibility:

**a. Legal and Regulatory Compliance:** Ensure compliance with relevant laws and regulations governing elections, data protection, and cybersecurity. Collaborate with legal experts to address legal challenges associated with online voting, such as jurisdictional issues and dispute resolution mechanisms.

**b. Stakeholder Engagement:** Engage with key stakeholders, including government agencies, election authorities, political parties, and civil society organizations, to garner support for the adoption of online voting. Conduct public awareness campaigns to educate voters about the benefits and security measures of the online voting system.

**c. Risk Management:** Identify potential risks and vulnerabilities associated with the online voting system, such as cyber attacks, technological failures, and voter coercion. Develop contingency plans and mitigation strategies to address these risks and ensure the integrity and reliability of the voting process.

### 4.1.5 Conclusion:

The feasibility study demonstrates that an online voting system using blockchain technology holds significant promise in enhancing the democratic process by providing a secure, transparent, and accessible platform for conducting elections. However, successful implementation requires careful consideration of technical, economical, and operational factors, as well as proactive measures to address potential challenges and risks. With proper planning, collaboration, and stakeholder engagement, the adoption of online voting systems can contribute to a more inclusive and trustworthy electoral system.

## 4.2 Software Requirement Specification

### 4.2.1 Data Requirement

#### 4.2.1.1 Voter Data

Personal Information: Name, Address, Date of Birth, Voter ID or Unique Identifier.

Authentication Credentials: Username, Password.

Voter Registration Status: Confirmation of voter eligibility, Registration date, Voting district or constituency information.

#### 4.2.1.2 Voting Data

Ballot Information: List of candidates or options for each contest, Contest titles and descriptions, Candidate details (e.g., name, party affiliation).

Vote Selections: Record of votes cast for each contest, Timestamp of when the vote was cast.

Digital Signatures: Signatures to validate the authenticity and integrity of the vote, Signature of the voter to ensure non-repudiation.

#### 4.2.1.3 Blockchain Data

Transaction Data: Details of each voting transaction stored on the blockchain, Transaction IDs, Hash values for data integrity verification.

Block Information: Block headers containing metadata, Hash of the previous block to maintain the blockchain's integrity.

#### 4.2.1.4 Audit and Verification Data

Audit Trail: Log of all voting activities, including registration, voting, and result declaration, Timestamps for each activity.

Verification Records: Records to facilitate post-election audits and verifications, Cryptographic proofs to ensure the integrity of the election process.

#### 4.2.1.5 Security and Access Control Data

Access Logs: Records of user access to the voting system, Login/logout timestamps, IP addresses and device information for authentication.

Security Keys and Certificates: Public and private keys for encryption and decryption, SSL certificates for secure communication.

#### 4.2.1.6 Configuration Data

Network Configuration: Details of blockchain network nodes, Configuration parameters for consensus algorithms.

System Settings: Voting system configuration parameters, Thresholds for consensus and validation rules.

Backup and Recovery Data: Backup schedules and procedures for system recovery, Data retention policies and archival mechanisms.

#### 4.2.1.7 Reporting and Analytics Data

Election Results: Aggregated vote counts for each candidate and contest, Summary reports and visualizations of election outcomes.

Voter Turnout Statistics: Analysis of voter participation rates.

### 4.2.2 Functional Requirement

#### 4.2.2.1 Voter Registration

Voter Registration Form: The system shall provide an online voter registration form. The form shall collect personal information, including name, address, and date of birth., The system shall verify voter eligibility based on registration criteria.

Authentication Mechanism: The system shall authenticate voters using unique identifiers, such as voter ID or biometric data. Voters shall be required to create authentication credentials (username and password) for access.

#### 4.2.2.2 Ballot Creation and Management

Ballot Generation: The system shall generate electronic ballots for each election or voting event. Ballots shall include contest titles, descriptions, and options for voting.

Contest Configuration: Administrators shall be able to configure contests and candidates for each ballot. The system shall allow for the addition, modification, and removal of contests and candidates.

#### 4.2.2.3 Voting Process

Access to Ballots: Registered voters shall have access to electronic ballots during the voting period. The system shall prevent multiple votes from the same voter for the same contest.

Vote Submission: Voters shall be able to select their choices for each contest and submit their votes securely. The system shall timestamp and record each vote on the blockchain for transparency and auditability.

#### 4.2.2.4 Blockchain Integration

Transaction Recording: The system shall record all voting transactions on the blockchain in a secure and immutable manner. Each voting transaction shall be associated with a unique transaction ID and cryptographic hash.

Consensus Mechanism: The system shall implement a consensus mechanism (e.g., proof-of-work) to validate and confirm transactions. Blockchain nodes shall participate in the consensus process to ensure the integrity of the distributed ledger.

#### 4.2.2.5 Results Tabulation and Reporting

Vote Counting: The system shall tally votes for each candidate and contest based on blockchain records. Results shall be computed and updated in real-time as new votes are recorded.

Result Presentation: The system shall generate summary reports and visualizations of election outcomes. Reports shall include aggregated vote counts, turnout statistics, and winner declarations.

#### 4.2.2.6 Security and Access Control

Access Management: The system shall enforce role-based access control for administrators, voters, and other users. Access permissions shall be granted based on user roles and responsibilities.

#### 4.2.2.7 System Administration

Administrative Dashboard: Administrators shall have access to a dashboard for managing system settings, users, and elections. The dashboard shall provide tools for monitoring system performance and resolving issues.

Audit and Logging: The system shall maintain audit logs of all voting activities, administrative actions, and system events. Logs shall be accessible to administrators for security monitoring and compliance purposes.

### 4.2.3 Performance Requirements

#### 4.2.3.1 System Response Time

Voter Registration: The system shall respond to voter registration requests within 5 seconds on average. Response time may vary based on server load but should not exceed 10 seconds under normal conditions.

Ballot Generation: The system shall generate electronic ballots for each election event within 2 seconds. Ballot generation time may increase slightly for complex ballots but should not exceed 5 seconds.

Vote Submission: The system shall acknowledge vote submissions instantly upon receipt. Confirmation messages should be displayed to voters within 1 second of submitting their votes.

#### 4.2.3.2 Blockchain Performance

Transaction Throughput: The system shall support a minimum transaction throughput of 100 transactions per second (TPS). Transaction processing capacity may be scaled dynamically based on network demand.

Consensus Latency: The consensus mechanism shall confirm transactions within 10 minutes on average. Confirmation time may vary based on network congestion but should not exceed 30 minutes under normal conditions.

#### 4.2.3.3 Scalability

Voter Capacity: The system shall accommodate large registered voters concurrently. Voter registration, ballot generation, and vote submission processes should scale horizontally to handle increasing demand.

Blockchain Scalability: The blockchain network shall scale to support increased transaction volumes without compromising performance. Horizontal scaling techniques such as sharding or sidechains may be employed to enhance network capacity.

#### 4.2.3.4 Availability and Reliability

System Uptime: The system shall maintain a minimum uptime of 99.9% excluding scheduled maintenance windows. Planned maintenance activities shall be communicated to users in advance to minimize disruption.

Fault Tolerance: The system shall be designed with redundancy and failover mechanisms to ensure high availability. Critical system components, including blockchain nodes and database servers, shall have backup systems in place to mitigate the impact of failures.

#### 4.2.3.5 Security Performance

Data Encryption Overhead: The system shall impose minimal overhead for data encryption and decryption processes. Encryption operations should not exceed 5% of CPU utilization to avoid performance degradation.

Access Control Checks: Access control checks and authentication processes shall be performed efficiently to minimize system overhead. Authentication response times should not exceed 100 milliseconds on average.

### 4.2.4 Maintainability Requirements

#### 4.2.4.1 Modular Architecture

Component-based Design: The system shall be developed using a modular architecture to facilitate easy maintenance and updates. Functionalities shall be divided into separate modules or components with well-defined interfaces.

Loose Coupling: Modules shall be loosely coupled to allow for independent development, testing, and deployment. Changes to one module should have minimal impact on other modules within the system.

#### 4.2.4.2 Documentation

Code Documentation: All source code shall be thoroughly documented to aid in understanding, modification, and troubleshooting. Comments and inline documentation shall be provided to explain code logic, algorithms, and data structures.

System Documentation: Comprehensive system documentation shall be maintained, including architecture diagrams, deployment guides, and user manuals. Documentation shall be kept up-to-date with any changes or enhancements to the system.

#### 4.2.4.3 Version Control

Source Code Management: The system shall utilize a version control system (e.g., Git) to track changes to source code and configuration files. Developers shall follow best practices for branching, merging, and version tagging to manage code changes effectively.

Change Management: Changes to the system shall be logged and tracked through a formal change management process. Change requests shall be evaluated, approved, and documented before implementation to ensure transparency and accountability.

#### 4.2.4.4 Scalability and Flexibility

Scalable Infrastructure: The system architecture shall be designed to scale horizontally and vertically to accommodate growth and increased demand. Scalability features such as load balancing, auto-scaling, and resource optimization shall be implemented where applicable.

Configuration Management: System configuration settings shall be managed centrally and stored in configuration files or databases. Configuration parameters shall be adjustable without requiring code changes to facilitate system customization and adaptation.

### 4.2.5 Security Requirements

#### 4.2.5.1 Access Control

User Authentication: The system shall enforce strong authentication mechanisms for users, including voters, administrators, and system operators. Authentication methods may include passwords, biometric verification, or multi-factor authentication (MFA).

Role-Based Access Control (RBAC): Access to system functionalities and data shall be restricted based on user roles and responsibilities. RBAC policies shall be defined and enforced to ensure that users have appropriate access permissions.

#### 4.2.5.2 Data Protection

Encryption: Sensitive data, including voter information, voting transactions, and system configurations, shall be encrypted during storage and transmission. Strong encryption algorithms and protocols shall be used to protect data confidentiality and integrity.

Anonymization: Personally identifiable information (PII) of voters shall be anonymized or pseudonymized to prevent unauthorized access and identity disclosure. Voter anonymity shall be maintained throughout the voting process to uphold privacy and confidentiality.

#### 4.2.5.3 Auditability and Logging

Audit Trails: The system shall maintain detailed audit trails of all user activities, system events, and voting transactions. Audit logs shall record timestamped information, including user actions, access attempts, and system changes.

Immutable Logging: Audit logs shall be stored in a tamper-evident manner using cryptographic hashing or blockchain technology. Once recorded, audit log entries shall be immutable and resistant to unauthorized modifications or deletions.

#### 4.2.5.4 System Integrity

Code Integrity: System components and software libraries shall be regularly scanned for vulnerabilities and compliance with security standards. Code integrity checks and validation processes shall be implemented to prevent unauthorized modifications or injections.

Configuration Management: System configurations shall be securely managed and protected from unauthorized changes or tampering. Configuration files shall be encrypted, and access permissions shall be restricted to authorized administrators only.

#### 4.2.5.5 Secure Communication

Transport Layer Security (TLS): All communications between system components, clients, and external services shall be encrypted using TLS/SSL protocols. Secure communication channels shall be established to prevent eavesdropping, tampering, or man-in-the-middle attacks.

Secure APIs: Application Programming Interfaces (APIs) exposed by the system shall be protected with strong authentication and authorization mechanisms. API endpoints shall be rate-limited, and access shall be restricted to authorized clients and applications.

## 4.3 SDLC Model Used

### 4.3.1 Agile Software Development Model with Iterative Prototyping:

**1. Planning Phase:**

**Project Initiation:** Define project objectives, scope, and requirements for the online voting system.

**Stakeholder Analysis:** Identify stakeholders, including students, faculty, election authorities, and IT team members.

**Initial Requirements Gathering:** Conduct interviews, surveys, and workshops to gather initial requirements and prioritize features.

**2. Development Phase:**

**Iteration 1: Minimum Viable Product (MVP) Development:**

Develop a basic version of the online voting system with essential features. Implement blockchain integration for vote recording and verification.

Focus on building a secure and user-friendly interface for casting votes.

**Iteration 2: Feedback and Enhancement:**

Gather feedback from stakeholders and users on the MVP.

Identify areas for improvement and additional features based on feedback.

Incorporate enhancements and iterate on the system design and functionality.

**3. Testing Phase:**

**Unit Testing:** Conduct unit tests to ensure the correctness of individual components and modules.

**Integration Testing:** Verify the integration of different system components, including blockchain integration, authentication mechanisms, and user interfaces.

Security Testing: Perform security assessments to identify vulnerabilities and ensure robustness against attacks, including penetration testing and code reviews.

**4. Deployment Phase:**

**Beta Testing:** Release the online voting system to a limited group of users for beta testing.

**User Acceptance Testing (UAT):** Allow stakeholders and end-users to test the system in a simulated environment and provide feedback.

**Gradual Rollout:** Deploy the system gradually, starting with a small-scale pilot and scaling up based on feedback and performance.

**5. Maintenance Phase:**

**Ongoing Support:** Provide ongoing support and maintenance for the deployed system, including bug fixes, security updates, and performance optimizations.

**Continuous Improvement:** Continuously gather feedback from users and stakeholders to identify opportunities for further enhancement and refinement.

**6. Risk Management:**

**Risk Identification:** Identify potential risks and uncertainties associated with the development and deployment of the online voting system.

**Risk Mitigation:** Develop risk mitigation strategies to address identified risks, such as security vulnerabilities, usability issues, and regulatory compliance.

**Contingency Planning:** Prepare contingency plans to mitigate the impact of unforeseen events or failures during the development and deployment process.

By adopting an Agile Software Development Model with Iterative Prototyping, the project team can effectively manage the complexity of developing an online voting system using blockchain technology. This approach allows for continuous feedback, collaboration, and

adaptation throughout the project lifecycle, leading to the successful delivery of a secure, transparent, and user-friendly voting system.

## 4.4 System Design

### 4.4.1 Data Flow Diagram

In the Level 0 Data Flow Diagram (DFD), the online voting system functions as the central process, facilitating smooth interactions among four main entities. Firstly, voters initiate the process by inputting their data, which is then verified by the system for successful login authentication. Similarly, candidates provide relevant data to participate in the electoral process. Administrators manage both candidates and voters, overseeing tasks like registration and system maintenance. Lastly, authorities interact with the system to access electoral results and monitor the voting process. The e-voting system serves as the core, orchestrating data flow to ensure integrity and transparency throughout the electoral process.

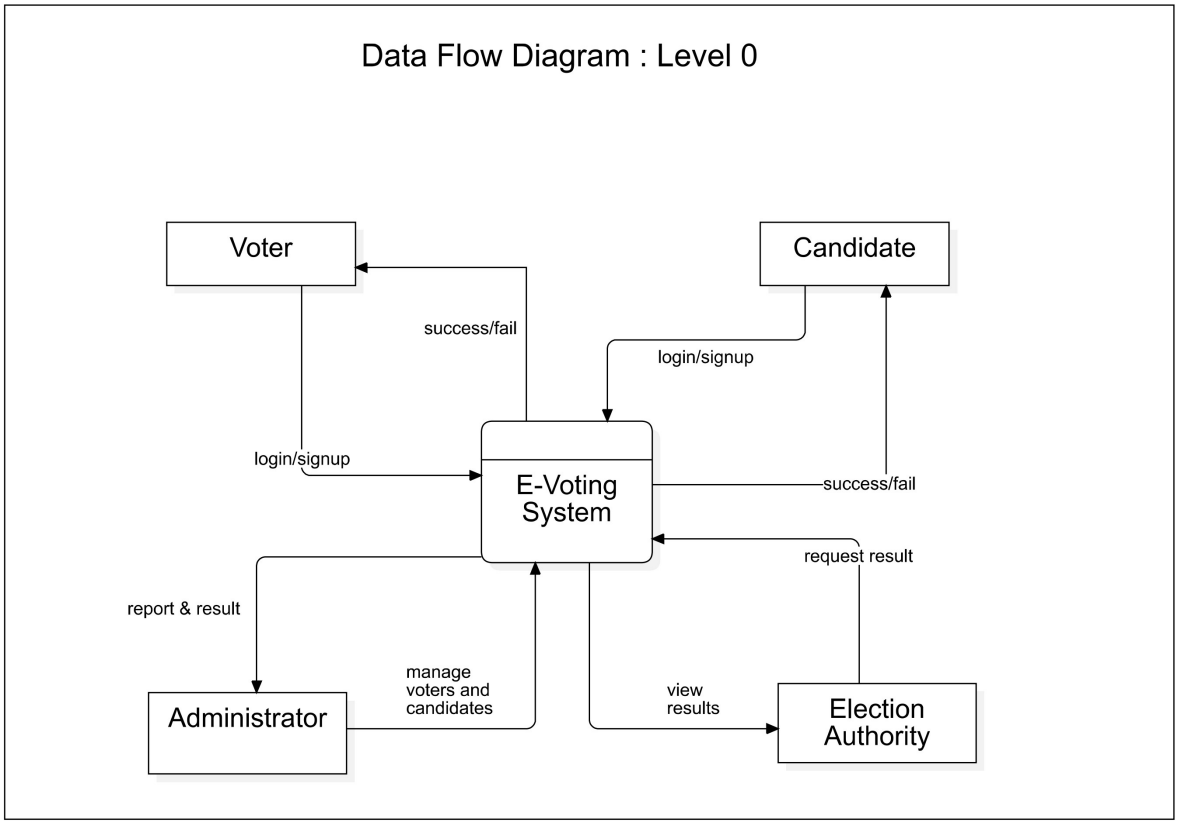



**Fig 4.1**
**DFD Level 0**

At level 1 of the Data Flow Diagram (DFD) for the online voting system, the main process "e-voting system" is divided into five subprocesses. The "Authentication" process verifies user credentials against stored data, granting access upon validation. "Voter/Candidate Registration" collects and stores user details for future reference. "Voting/Polling" enables registered voters to cast votes securely, preventing duplicate or fraudulent votes. "Result Calculation" computes election results based on tallied votes, securely storing outcomes. "Voting Management" oversees the entire process, managing tasks like scheduling, performance monitoring, and issue resolution. Throughout, entities like Voter, Candidate, Administrator, and Authority interact, supported by data stores for voting details and user information.

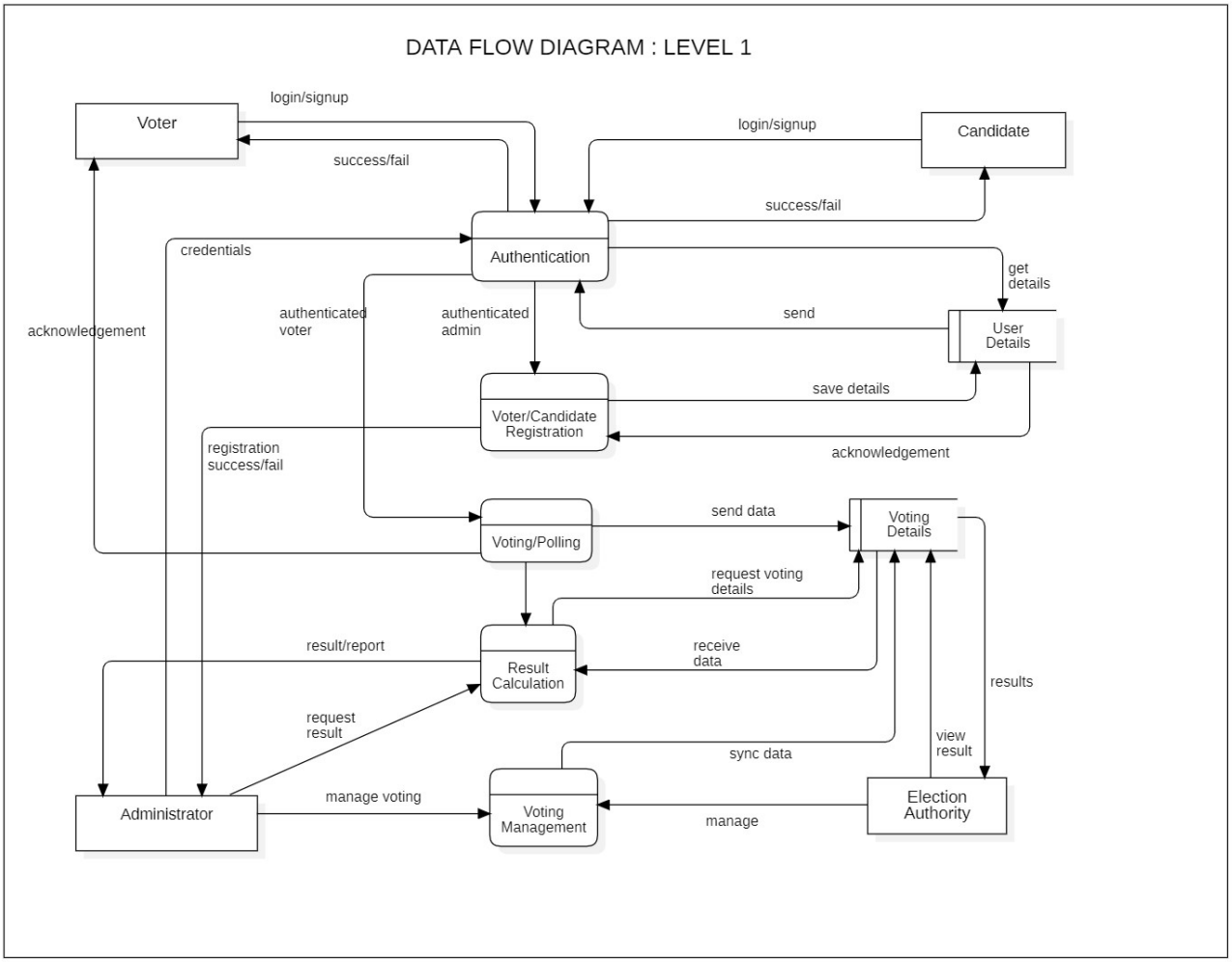



**Fig 4.2**

**DFD Level 1**

### 4.4.2 Use Case Diagrams

The use case diagram for the online voting system outlines three primary actors: Voter, Administrator, and Election Authority. Additionally, there's a secondary actor, Election Authority, which interacts indirectly to view and release results. The main functionalities include Authentication, View Candidate, Cast Vote, Manage Voting (Admin), Add/Delete/Modify Candidates/Voters, View Results (by Authority), and Release Results (by Authority). These use cases allow actors to log in, view candidate lists, cast votes securely, manage voting processes, and oversee election results. Administrators can add, delete, or modify candidate and voter details, while Election Authorities monitor and release election results to ensure transparency.

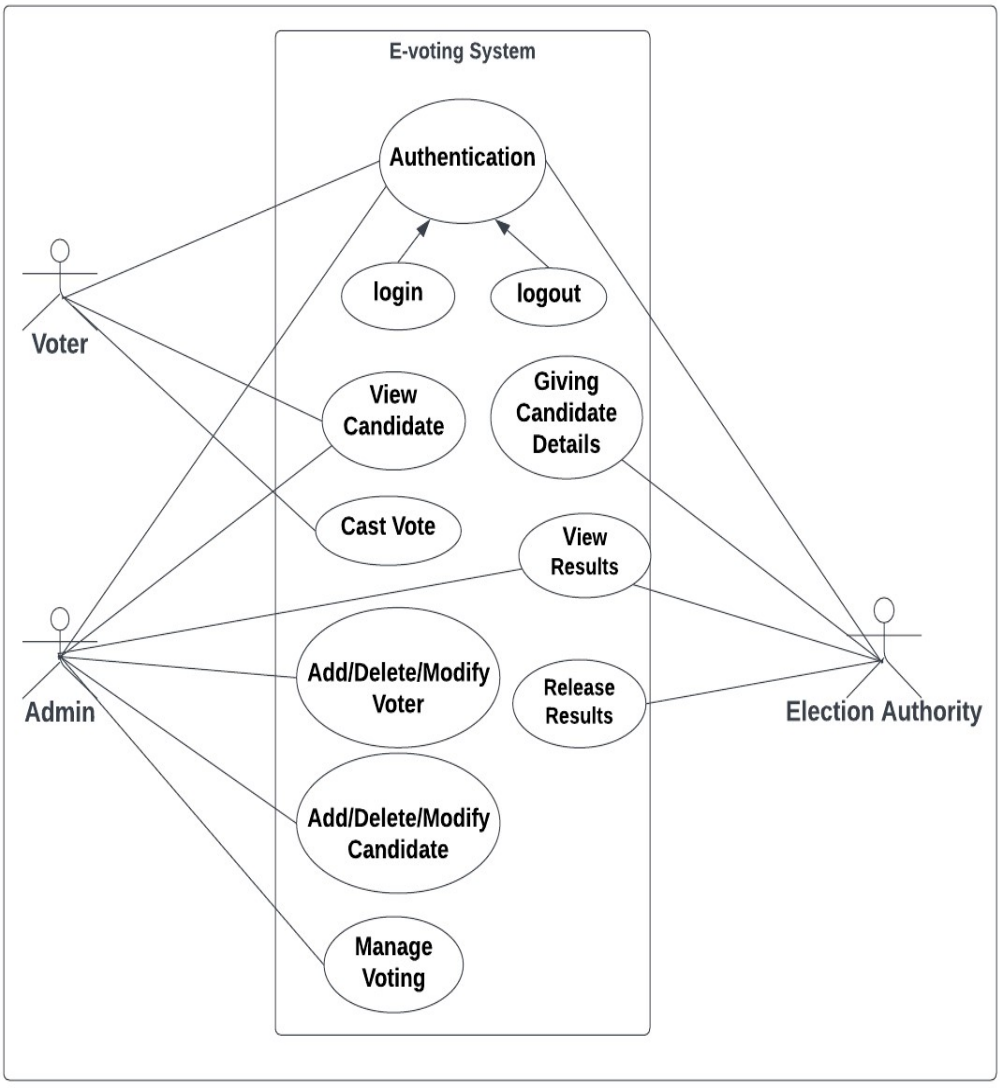



**Fig 4.3**

**Use Case Diagram**

## 4.5 Database Design

The ER diagram depicts an online voting system with four main entities: Voter, Candidate, Admin, and Election. Each entity has specific attributes and relationships. Voters can vote for one or more candidates, while candidates can participate in one or more elections. Admins manage both voters and candidates, with each admin overseeing multiple voters and candidates. Elections have start and end times, and both voters and candidates can participate in multiple elections. Overall, the diagram outlines the structure and connections within the e-voting system, facilitating efficient management and participation in electoral processes.

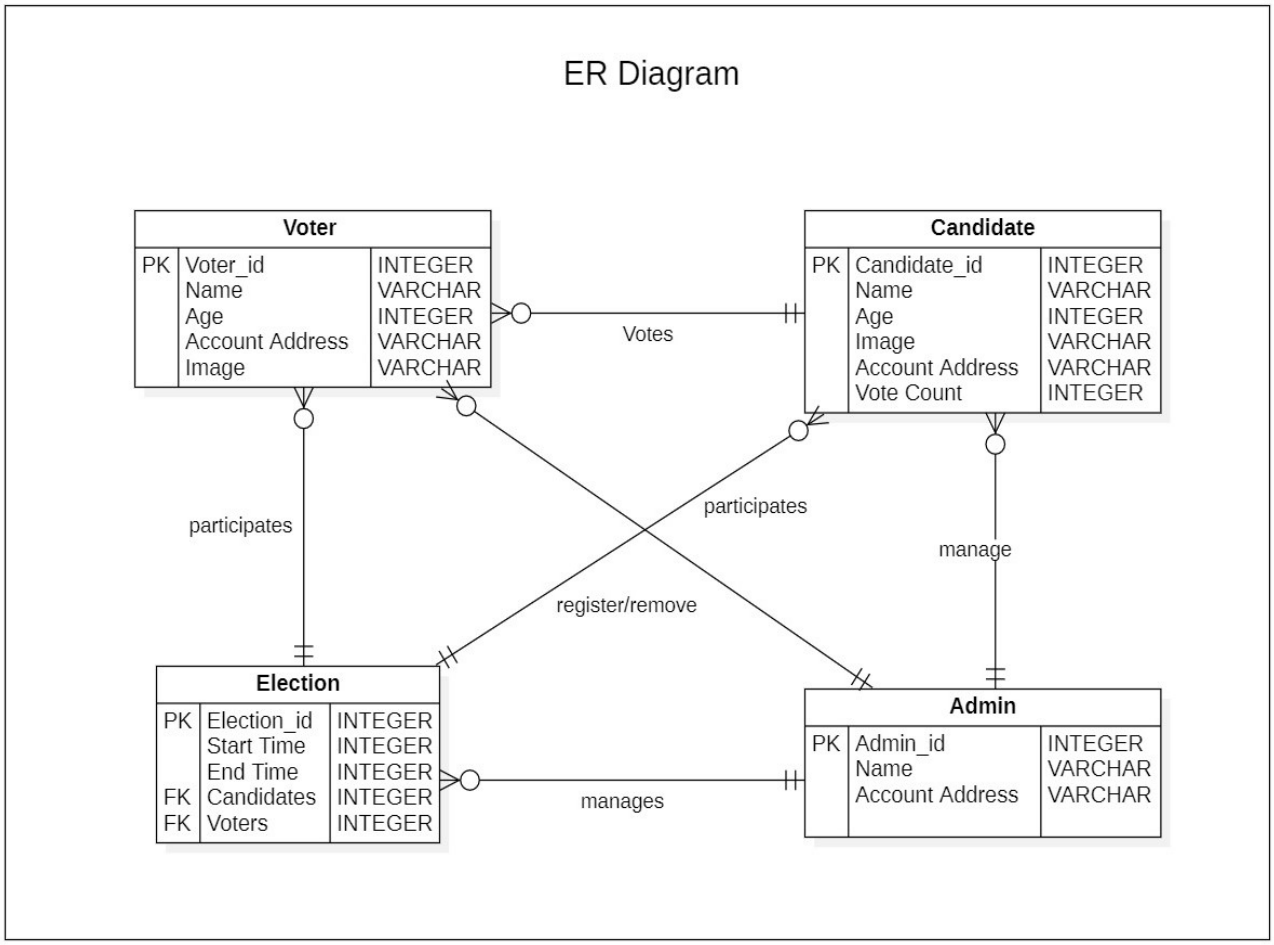



**Fig 4.4**

**ER Diagram**

# CHAPTER 5

# IMPLEMENTATION

## 5.1 Introduction Tools and Technologies Used

**1. Solidity:** A statically-typed curly-braces programming language designed for developing smart contracts that run on Ethereum.

**2. Hardhat:** Hardhat is a development environment for Ethereum software. It consists of different components for editing, compiling, debugging and deploying your smart contracts and dApps, all of which work together to create a complete development environment.

**3. IPFS (InterPlanetary File System):** The IPFS is a set of composable, peer-to-peer protocols for addressing, routing, and transferring content-addressed data in a decentralized file system.

**4. Metamask:** MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

**5. Next.js:** Next.js is an open-source web development framework created by the private company Vercel providing React-based web applications with server-side rendering and static website generation.

**6. Node.js:** Node.js is a free, open-source, cross-platform JavaScript runtime environment that lets developers create servers, web apps, command line tools and scripts.

**7. Blockchain:** This is not a specific technology but rather a distributed ledger technology on which cryptocurrencies and decentralized applications are built. Ethereum is one of the most popular blockchains for developing decentralized applications due to its support for smart contracts.

**8. Git/GitHub:** Version control system and a web-based hosting service for Git repositories, respectively. They are essential tools for collaborative software development, allowing developers to track changes, manage codebases, and coordinate contributions.

# CHAPTER 6

# TESTING AND MAINTENANCE

## 6.1 Testing Techniques and Test Cases Used

### 6.1.1 In Scope

This shows the aspects of the E-Voting System that are within the scope of our testing efforts. It includes the following:

**Voting Interface:** Testing the user interface to ensure that it is user-friendly, accessible, and accurately captures voter choices.

**Vote Encryption and Decryption:** Ensuring the cryptographic processes used to secure votes are functioning correctly.

**Vote Recording:** Validating that each vote is accurately recorded on the blockchain ledger.

**Security Measures**: Verifying the effectiveness of security measures to protect against unauthorized access.

**Performance**: Assessing the system's responsiveness and scalability to handle a significant volume of votes.

**Usability:** Evaluating the overall user experience and accessibility of the system.

### 6.1.2 Out of Scope

For our E-Voting System, the following are out of scope:

**No. of voters:** Only limited number of entities can be tested.

**Blockchain Technology**: The core blockchain technology itself, as it should have undergone extensive testing during its development.

**Hardware Infrastructure:** The physical hardware infrastructure supporting the system is out of scope.

**Network Infrastructure:** The broader network infrastructure is not within our testing purview.

### 6.1.3 Quality Objective

Our quality objectives are:

**Accuracy:** Ensuring that each vote is recorded and counted accurately.

**Security:** Guaranteeing the integrity, confidentiality, and availability of the voting data.

**Usability:** Creating a user-friendly system that is accessible to a broad range of voters.

**Performance:** Ensuring the system can handle a significant load without degradation.

### 6.1.3 Roles and Responsibilities

Detail description of the Roles and responsibilities of team members

Test Manager (Ashish Kumar Gupta)

Tester (Ashish Kumar Gupta) – Tested the test cases.

Developers (Ashish Kumar Gupta, Saurabh Pundir, Aditya Aggarwal) - Addressed and resolved issues identified during testing.

Project Manager (Mr. Akash Goel) - Oversee the project's progress and ensure alignment with testing efforts.

### 6.1.4 Test Methodology

**Overview**

For our E-Voting System project, we have adopted the Waterfall test methodology. The choice of this methodology is driven by several key factors specific to our project's requirements and characteristics:

As our requirements are clearly defined and stable we are using Waterfall methodology.

The voting process is subject to strict regulations, and a Waterfall approach allows for thorough planning and documentation to ensure compliance with legal and security requirements.

Waterfall provides a structured approach.

### 6.1.5 Test Levels

Following are the testing levels that are defined based on the case of the E-Voting System:

**Unit Testing:** Ensuring that the all the modules are working correctly.

**Integration Testing:** Testing that all the integrated modules are working as expected.

**System Testing:** Evaluating the entire system to verify its correctness and compliance with election regulations.

**User Acceptance Testing (UAT):** Allowing end-users, including election officials and voters, to validate the system for usability and suitability.

### 6.1.6 Suspension Criteria and Resumption Requirements

**Suspension Criteria:** If a critical security vulnerability is discovered during requirements testing, further testing may be suspended until the issue is resolved.

**Resumption Criteria:** In the case of the security vulnerability, testing can resume when the issue is fixed, and the system is confirmed secure.

### 6.1.7 Test Completeness

All requirements are met.

Compatibility: Software is compatible with other platforms, browsers, devices, OS.

100% test coverage

All Test cases executed

All open bugs are fixed or will be fixed in next release.

### 6.1.8 Manual Testing

**Table no. 6.1**

**Mannual Testing**

| Test_Case_ID | Test Case Objective | Pre Requisite | Input Data | Expexted Output | Actual Output | Status |
|---|---|---|---|---|---|---|
| TC_01 | Sign in using MetaMask | MetaMask wallet account | Account Password | Logged in | logged in | PASS |
| TC_02 | Test Image upload to IPFS using API | System must be connected to internet | Image | Image Uploaded | Image Uploaded | PASS |
| TC_03 | Retrieving uploaded image from IPFS | System must be connected to internet | | Image Retrieved | Image Retrieved | PASS |
| TC_04 | Registering Candidate & Connecting with Smart Contract | User must be logged in with admin account | Details of candidate & unique address | Candidate registered | Candidate registered | PASS |
| TC_05 | Registering Voter | User must be logged in with admin account | Details of voter & unique address | Voter registered | Voter registered | PASS |
| TC_06 | Voting as Voter | Must be registered by admin | | Voted | Voted | PASS |
| TC_07 | Voting again | Must be voted already | | You have already voted | You have already voted | PASS |

### 6.1.9 Automation Testing

**Test Case 1: Sign In Using Metamask**

**Test Description:** This scenario evaluates the functionality of signing into the E-Voting System using MetaMask, a popular Ethereum wallet and gateway to blockchain applications.

**Steps:**

Open the E-Voting System application.

Click on the "Sign In" option.

Select "Sign in using MetaMask."

Connect the MetaMask extension.

Verify successful sign-in and access to the user's account.

**Expected Result:** The user can sign in using MetaMask, and their account is accessible within system.

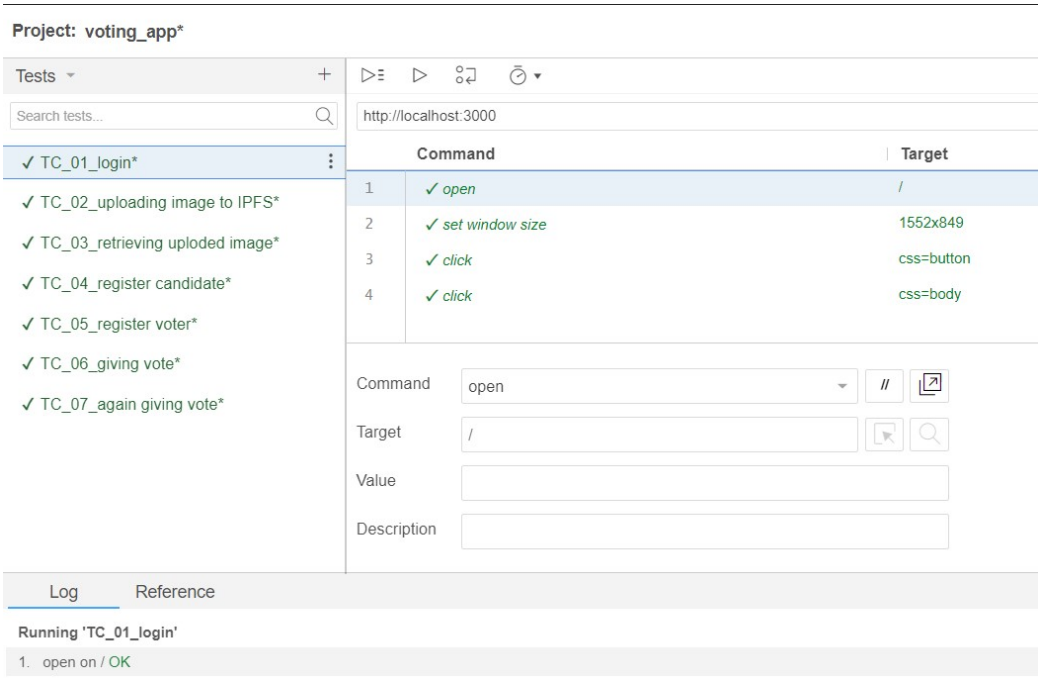



**Fig 6.1**

**AutomationTesting**

## Logs:

Running 'TC_01_login'20:47:36

1. open on / OK20:47:36

2. setWindowSize on 1552x849 OK20:47:37

3. click on css=button OK20:47:37

4. click on css=body OK20:47:39

'TC_01_login' completed successfully20:47:39

**Test Case 2: Test Image Upload to IPFS Using API:**

**Test Description:** This scenario examines the capability of the system to upload an image to IPFS via an API.

Test Steps:

Log in to the E-Voting System.

Navigate to the "Candidate Registration" section.

Upload an image using the upload button.

Confirm successful image upload.

**Expected Result:** The system allows users to upload images to IPFS through the IPFS API, and the image is successfully uploaded.

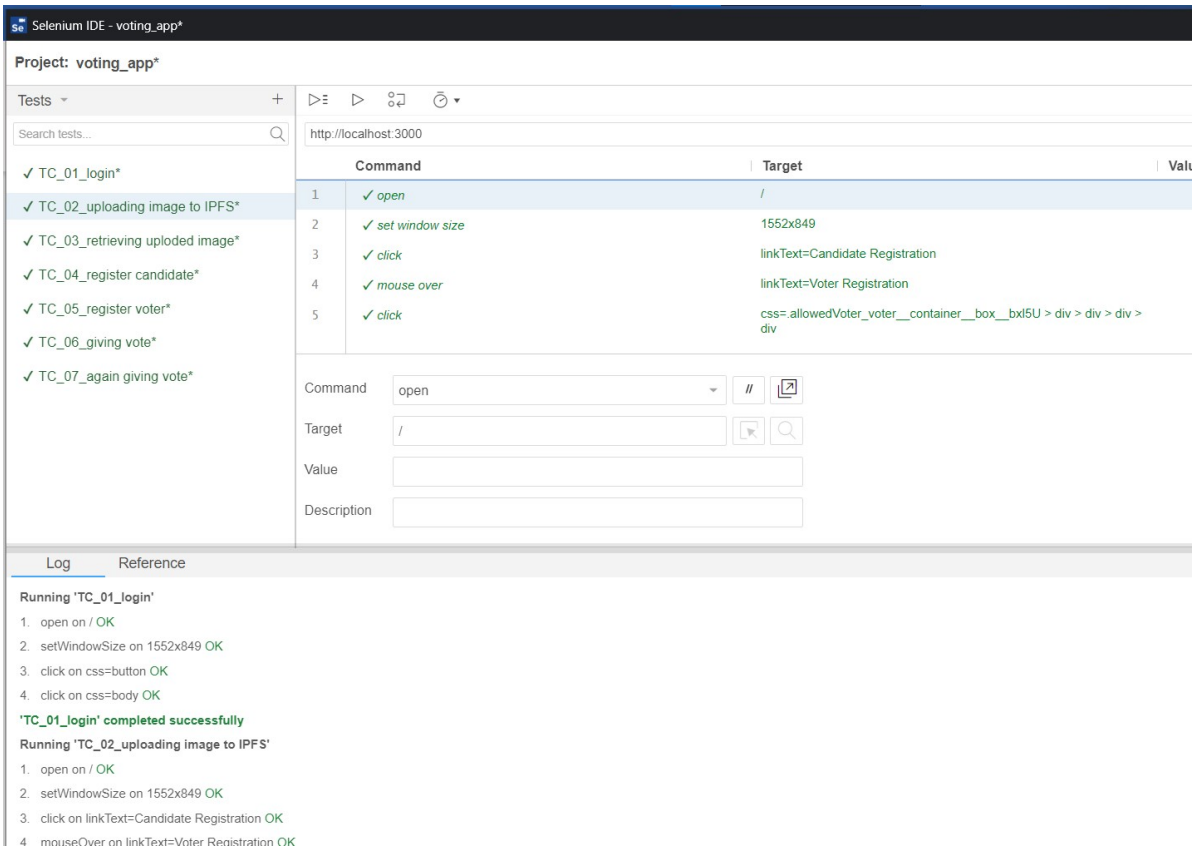



**Fig 6.2**

**Test Case 2**

**Test Case 3: Retrieving Uploaded Image from IPFS (after upload automatically)**

**Test Description:** This scenario tests the system's ability to retrieve an image previously uploaded to IPFS.

**Test Steps:**

Upload the image to the IPFS.

It will automatically retrieve and show the image.

Verify that the correct image is displayed.

**Expected Result:** The system successfully retrieves and displays the uploaded image from IPFS.

**Test Case 4: Registering Candidate & Connecting with Smart Contract**

**Test Description:** This scenario assesses the system's functionality to register a candidate and establish a connection with the underlying Smart Contract.

**Test Steps:**

Log in to the E-Voting System as an administrator.

Access the "Candidate Registration" section.

Register a candidate, providing relevant details and uploading image.

Confirm the transaction process.

**Expected Result:** The system successfully registers the candidate and establishes a connection with the Smart Contract, allowing the candidate to participate in the election.

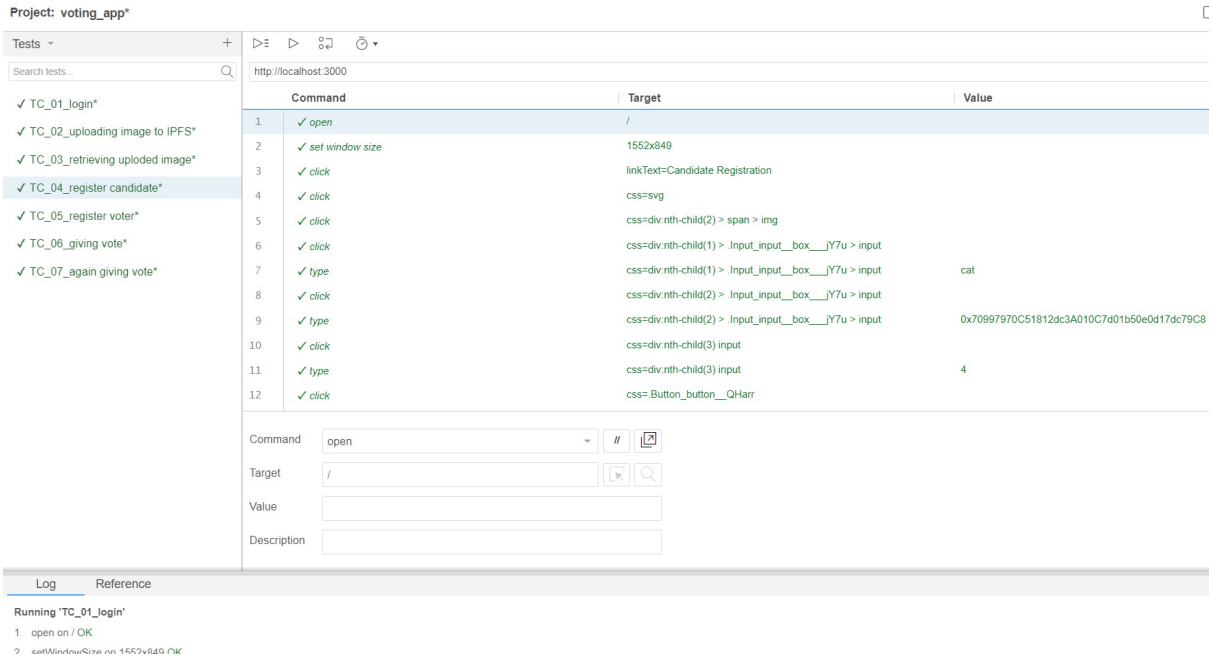



**Fig 6.3**

**Test Case 4**

**Test Case 5: Registering Voter**

**Test Description:** This scenario evaluates the system's capability to register voters for the election.

**Test Steps:**

Log in to the E-Voting System as an administrator.

Navigate to the "Voter Registration" section.

Register a voter by entering their details.

Verify that the voter's registration is recorded in the system.

**Expected Result:** The system registers the voter, making them eligible to participate in the election.

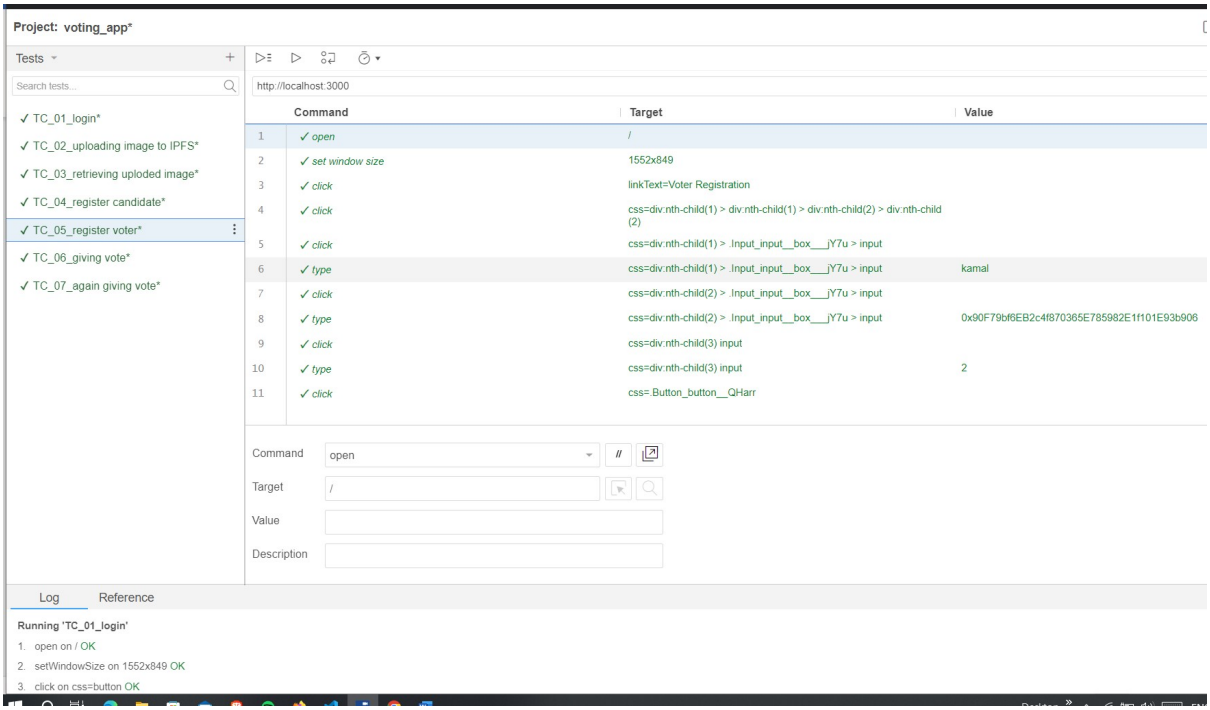



**Fig 6.4**

**Test Case 5**

**Test Case 6: Voting as Voter**

**Test Description:** This scenario evaluates the voting process for a registered voter.

**Test Steps:**

Log in as a registered voter.

Go to homepage of web application.

Cast a vote for a candidate by clicking vote button.

Verify that the vote is recorded in the system.

**Expected Result:** Registered voters can cast their votes successfully, and the system records their choices.

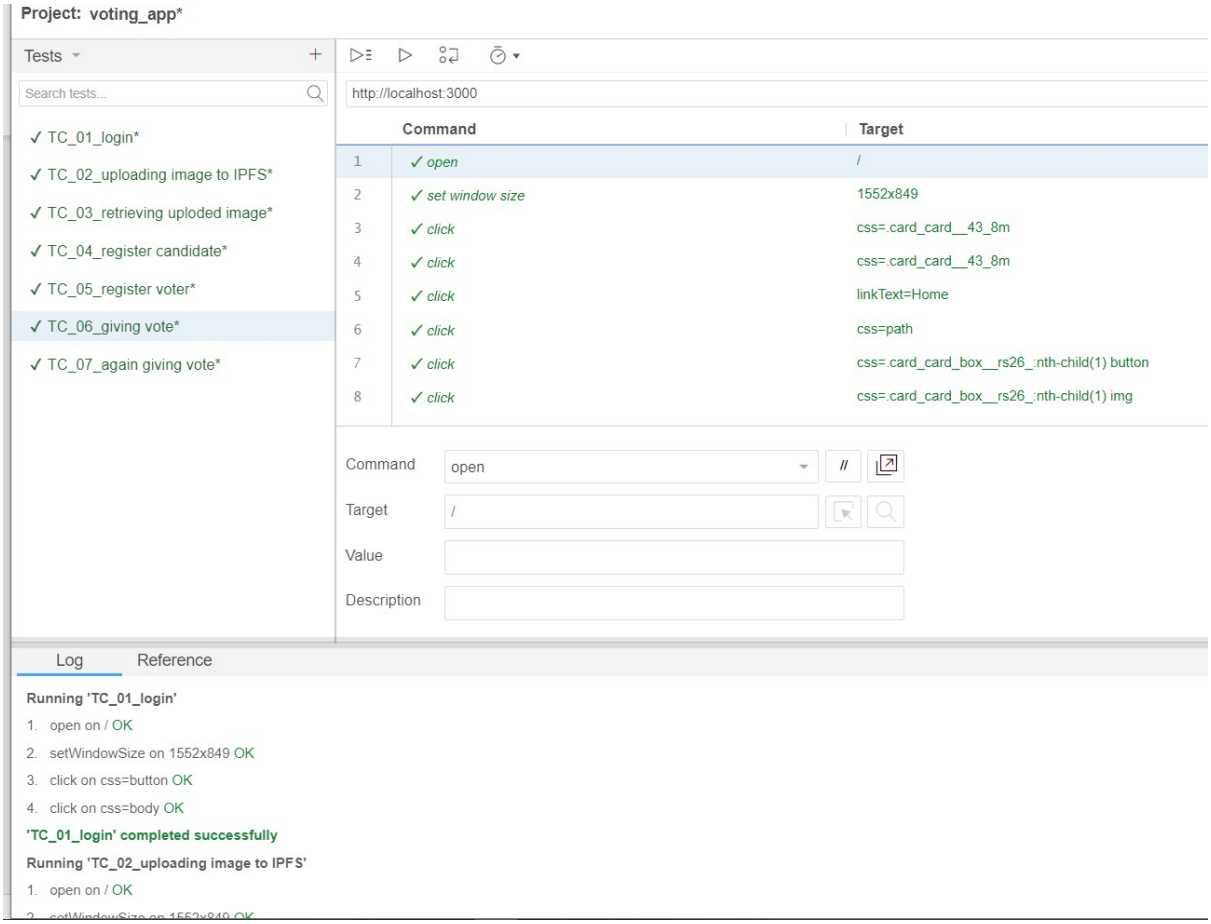



**Fig 6.5**

**Test Case 6**

## Test Case 7: Voting Again

**Test Description:** This scenario verifies the system's ability to prevent a voter from casting multiple votes.

**Test Steps:**

Log in as a registered voter.

Cast a vote for a candidate.

Attempt to vote again using the same voter account.

Confirm that the system prevents the voter from casting multiple votes.

**Expected Result:** The system should restrict voters from casting multiple votes, ensuring the integrity of the election process.

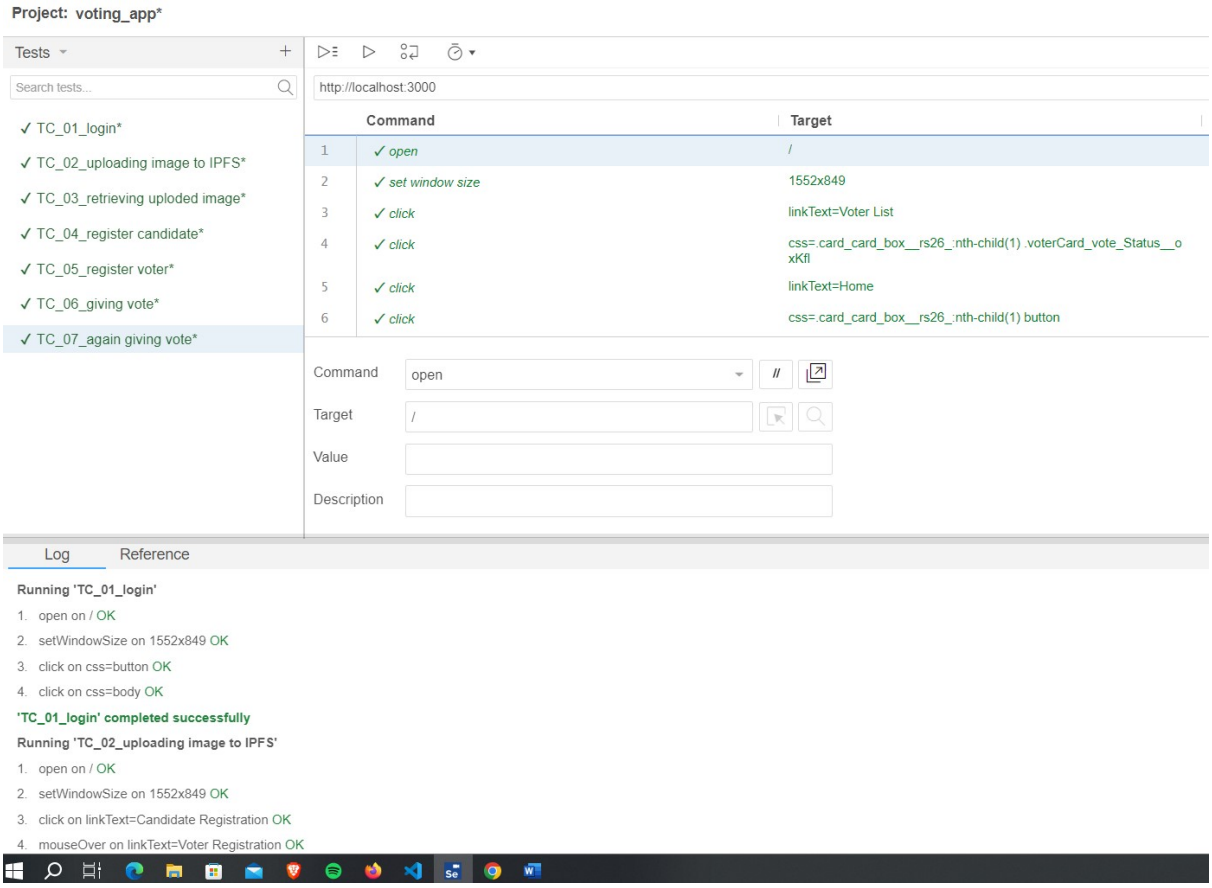



**Fig 6.6**

**Test Case 7**

## Testing Tools

Selenium IDE, Browser (Firefox or chrome)

## Test Environment

Following software's are required in addition to client-specific software.

Windows 10 and above, Browser, Microsoft Visual Studio

# CHAPTER 7

# RESULTS AND DISCUSSIONS

## 7.1 Description of Modules with Snapshots

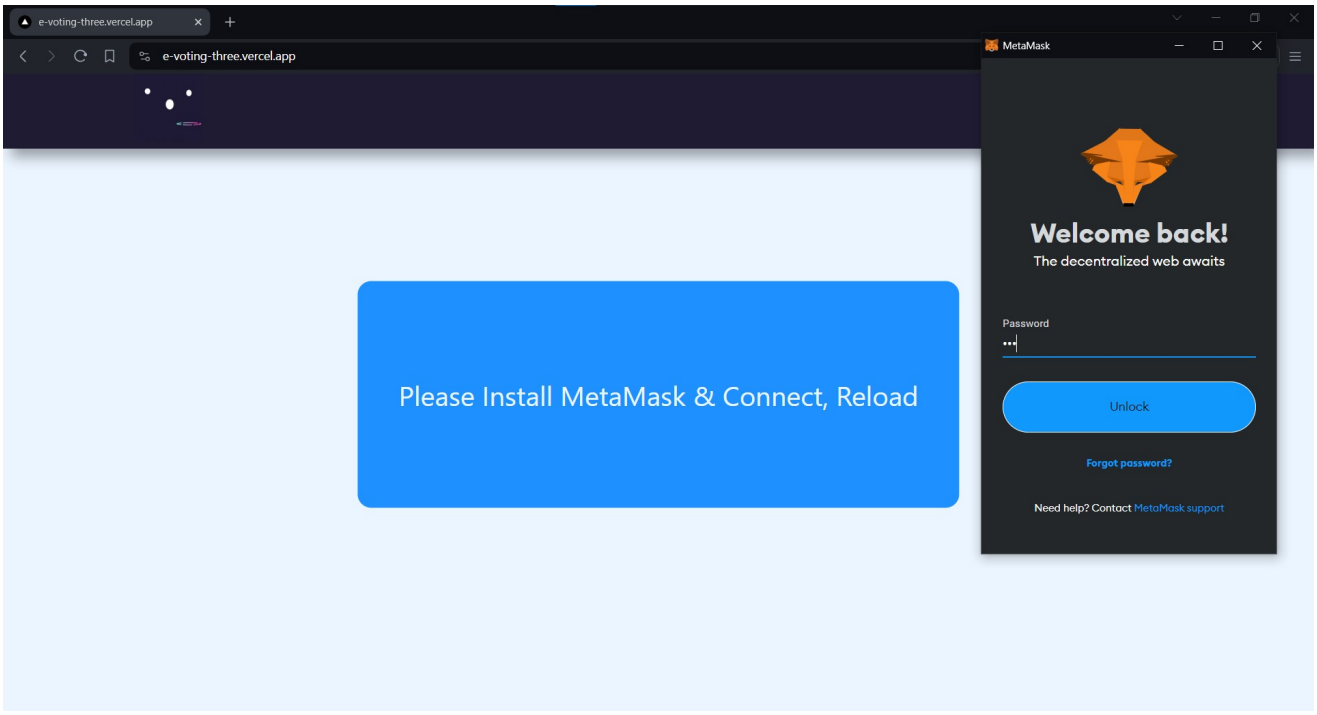



**Fig 7.1**

**Homepage and Metamask Login**

The homepage displays the login screen, which requires the user to log in to the voting system with a MetaMask Account. By logging in with the MetaMask account, the user will be able to access the UI.

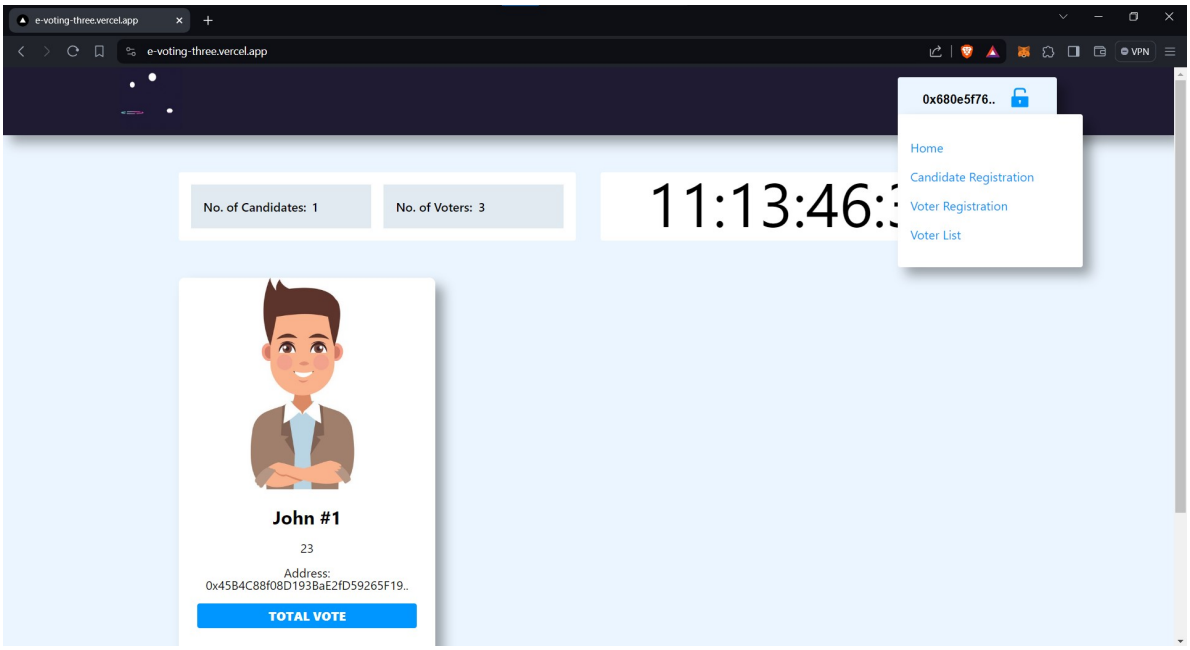



**Fig 7.2**

**User Interface**

This is the main UI of the app, which displays the candidates, the number of voters, and the candidate information.

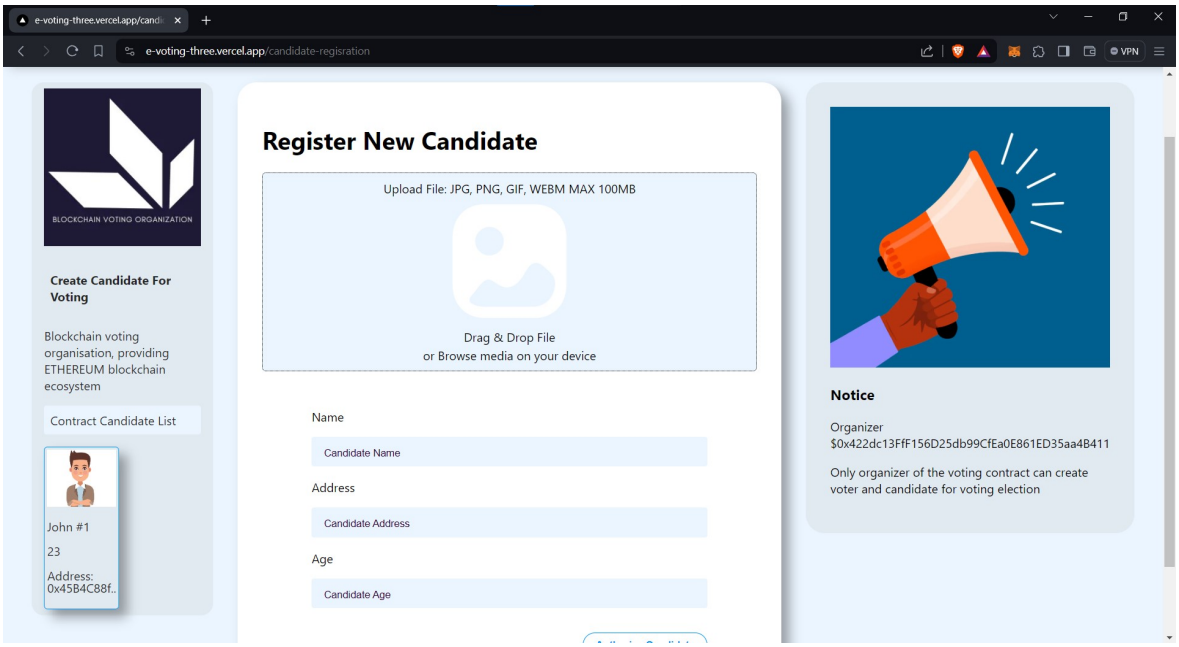



**Fig 7.3**

**Candidate Registration**

This is the candidate registration page, which includes a form for entering name, account address, age, and image upload.

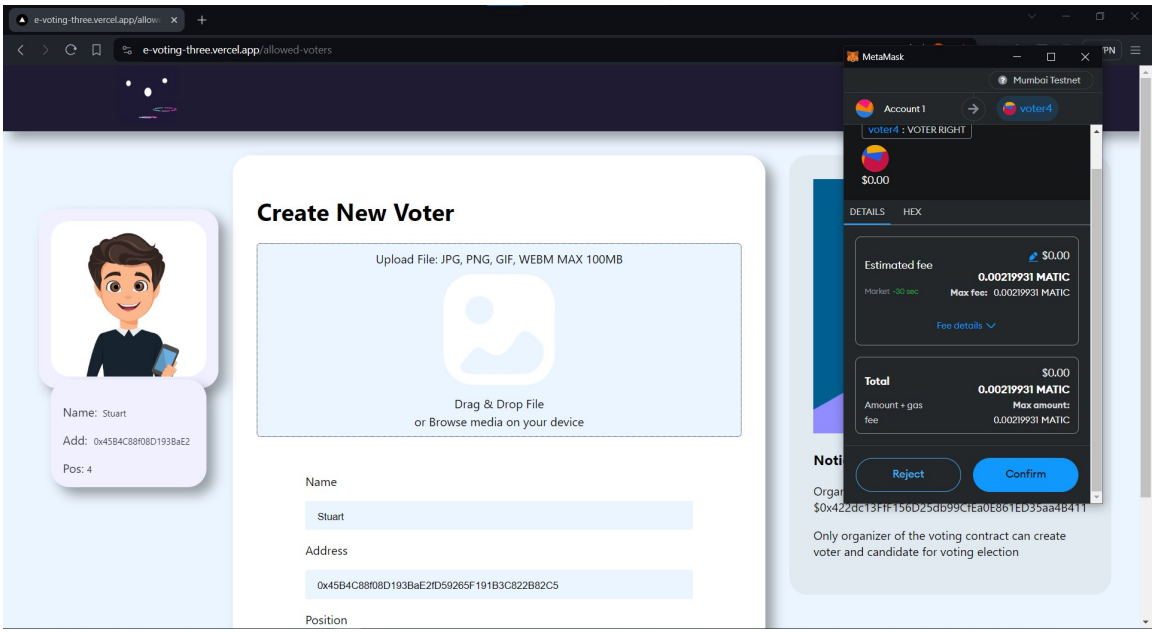



**Fig 7.4**

**Voter Registration**

Voter registration is the same as candidate registration.

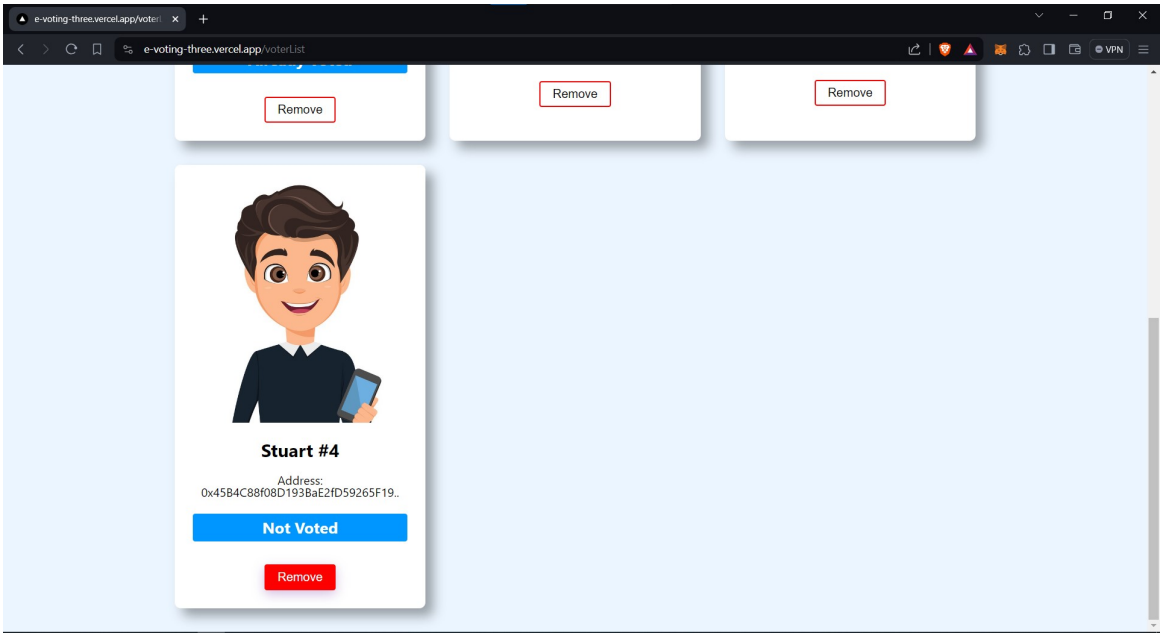



**Fig 7.5**

**Voter List**

This shows the voter list and their status, indicating whether they have voted or not.

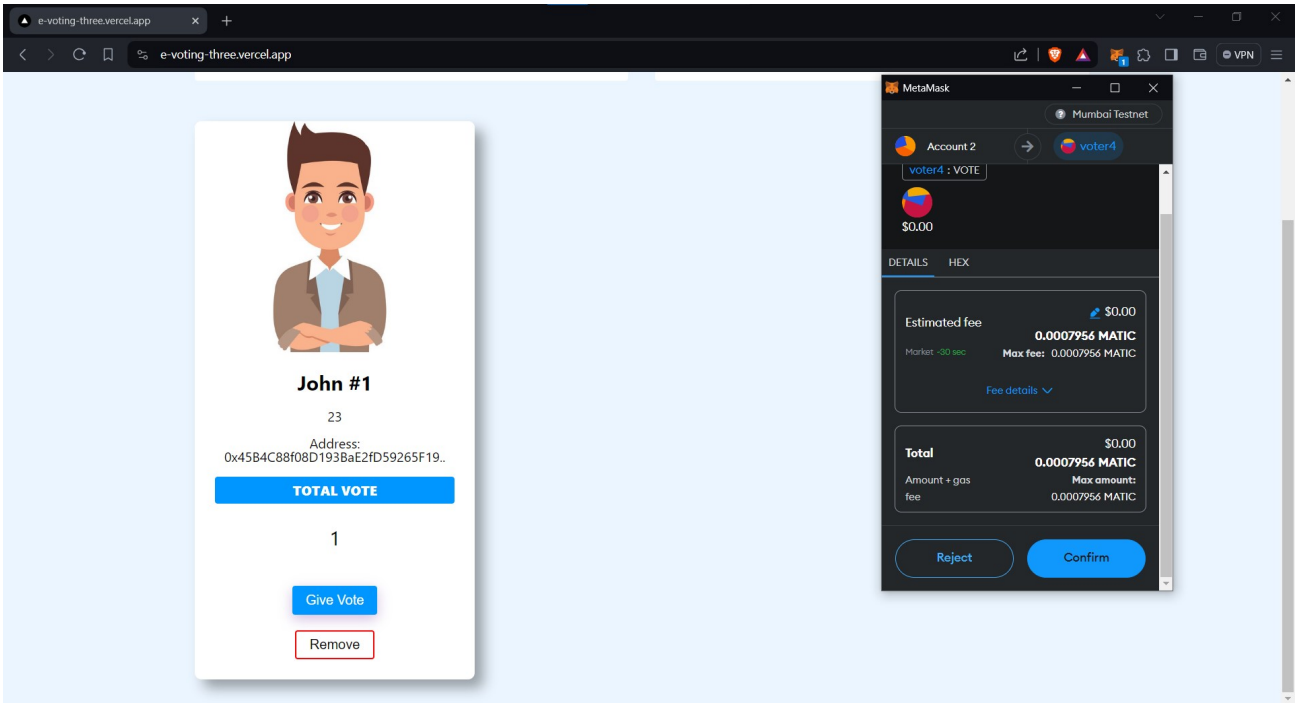



**Fig 7.6**

**Vote Casting**

In this image, voting is being conducted, and transactions are completed with MetaMask.

## 7.2 Key findings of the project

**1. Security Enhancement:** One of the primary findings would likely be the enhanced security provided by blockchain technology. The decentralized and immutable nature of the blockchain ensures that votes are securely recorded and tamper-proof, reducing the risk of fraud or manipulation.

**2. Transparency and Trust:** Implementing blockchain in the voting process increases transparency by allowing all participants to verify the integrity of the election results. This transparency fosters trust among voters and stakeholders in the fairness of the voting system.

**3. Cost Efficiency:** Blockchain-based voting systems have the potential to reduce costs associated with traditional voting methods, such as printing ballots, manual vote counting, and transportation of paper ballots. This could be a significant finding for stakeholders interested in optimizing election processes.

**4. Improved Accessibility:** Online voting systems can improve accessibility for voters, especially those with mobility issues or living in remote areas. By enabling voters to cast their

votes remotely via the internet, blockchain-based voting systems can increase voter turnout and participation.

**5. Challenges and Limitations:** Key findings may also highlight challenges and limitations faced during the implementation of the online voting system. These could include scalability issues, regulatory hurdles, cybersecurity concerns, and ensuring inclusivity and accessibility for all voters.

**6. User Feedback and Satisfaction:** Gathering feedback from users who participated in the online voting process can provide valuable insights into user experience, satisfaction levels, and areas for improvement. Positive feedback could indicate successful adoption and acceptance of the new voting system.

**7. Potential for Future Expansion:** If the project is successful, key findings may include insights into the potential for future expansion or adoption of blockchain technology in other voting processes or public sector applications.

## 7.3 Brief Description of Database with Snapshots

IPFS is a decentralized protocol designed to create a peer-to-peer network for storing and sharing hypermedia content. Unlike traditional centralized storage systems, where data is stored on a single server or a group of servers controlled by a central authority, IPFS distributes data across a network of nodes. Each piece of data is assigned a unique cryptographic hash, which serves as its address on the IPFS network.

In the context of an application, IPFS can be used to store various types of data, including text, images, videos, and documents. When data is uploaded to IPFS, it is broken down into smaller chunks, encrypted, and distributed across multiple nodes in the network. This decentralized approach to storage offers several advantages.

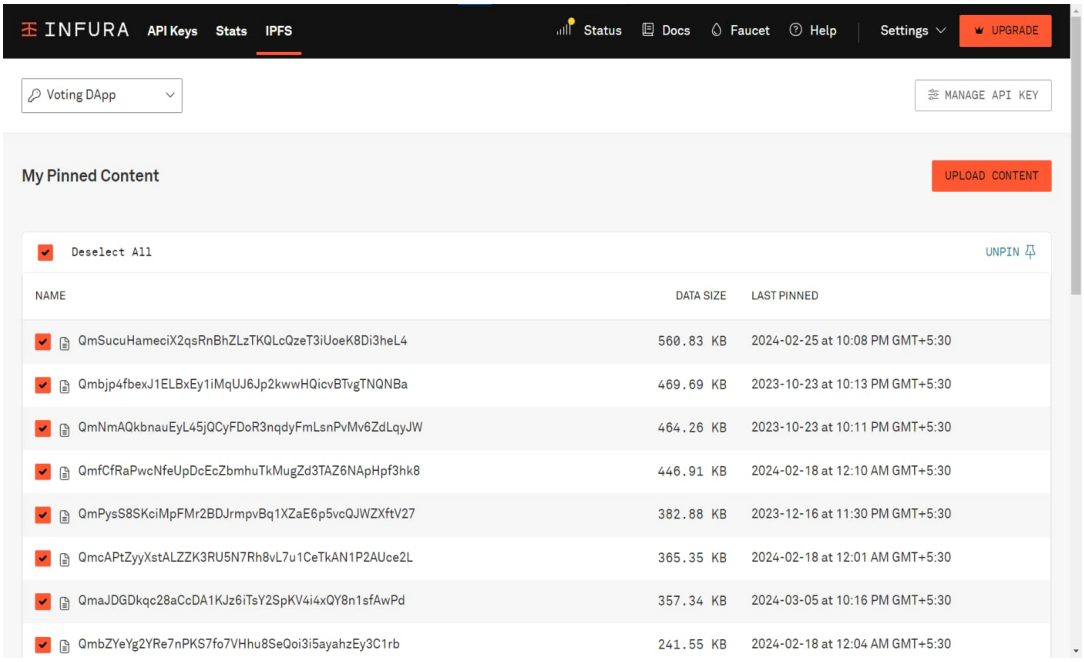



**Fig 7.7**

**IPFS Offchain storage**

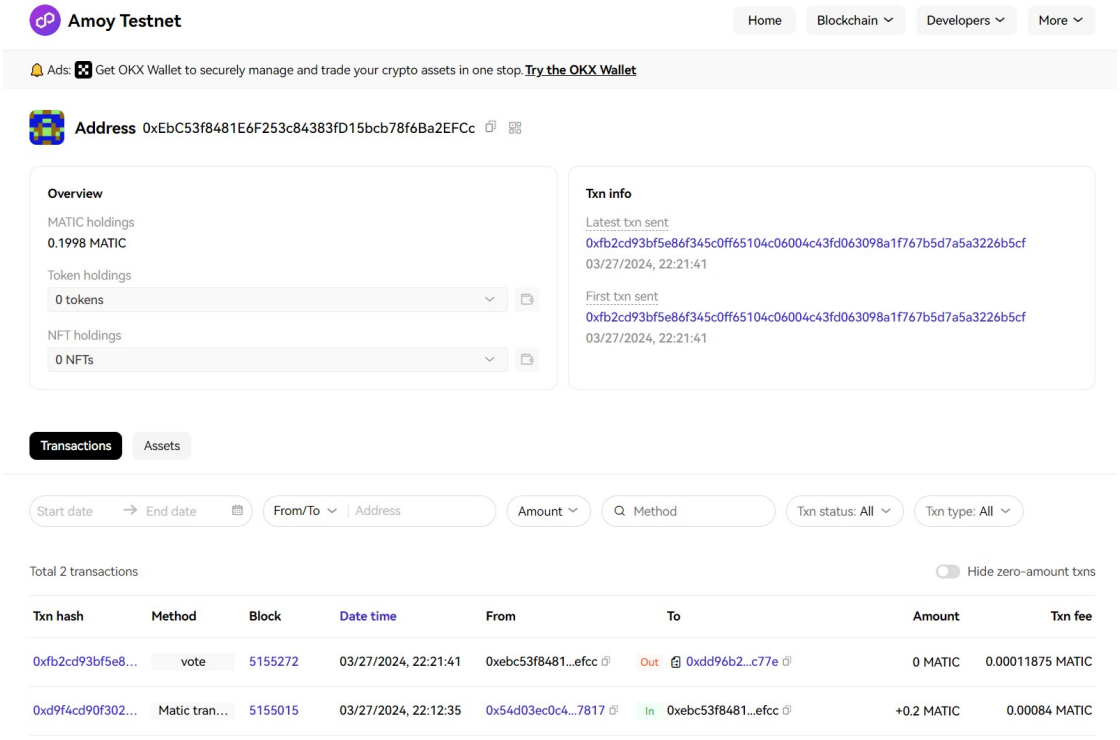



**Fig 7.8**

**Blockchain showing transaction done by single account**

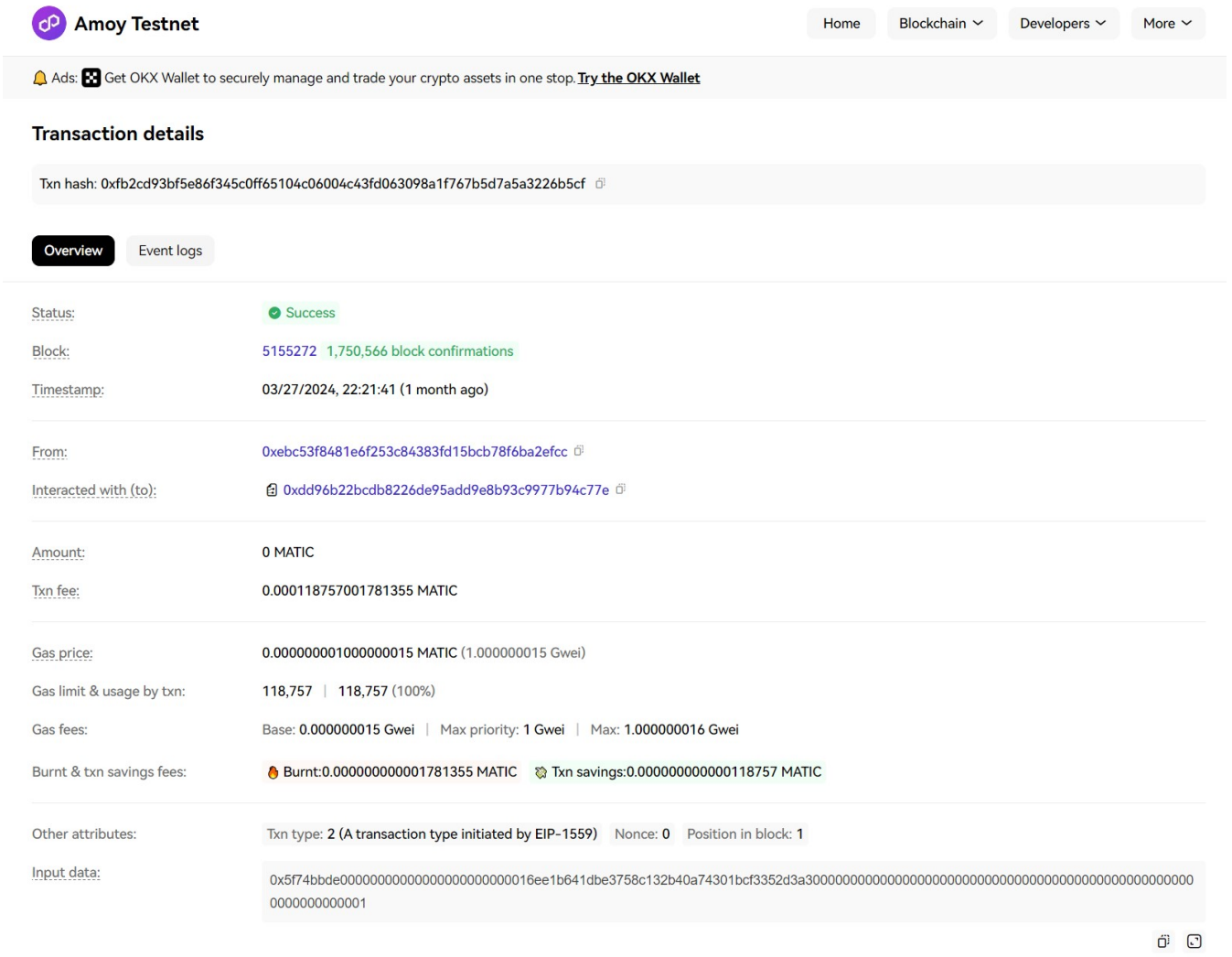



**Fig 7.9**

**Details of single transaction**

# CHAPTER 8
# CONCLUSION AND FUTURE SCOPE

## CONCLUSION

In conclusion, the utilization of blockchain technology in online voting systems presents a promising avenue for enhancing the security, transparency, and trustworthiness of electoral processes. By leveraging the immutable and decentralized nature of blockchain, we can mitigate many of the vulnerabilities associated with traditional voting methods, such as tampering and manipulation of results. However, while the potential benefits are evident, challenges remain in terms of scalability, accessibility, and regulatory frameworks. Moving forward, continued research, collaboration between technologists and policymakers, and pilot implementations will be essential in realizing the full potential of blockchain-based online voting systems. Despite the complexities involved, the pursuit of secure and inclusive democratic processes through innovative technologies like blockchain remains imperative for the advancement of society.

## FUTURE SCOPE

The future scope for online voting systems using blockchain technology holds promise in addressing longstanding issues of security, transparency, and accessibility in electoral processes. Further research could focus on enhancing the scalability and efficiency of blockchain-based voting systems to accommodate large-scale elections, exploring innovative cryptographic techniques to ensure voter privacy without compromising the integrity of the vote, and developing user-friendly interfaces to facilitate widespread adoption among diverse demographics. Additionally, there is a need for rigorous testing and validation of blockchain voting systems in real-world election scenarios to assess their effectiveness, reliability, and resilience against potential threats or vulnerabilities. Furthermore, future efforts may concentrate on the establishment of regulatory frameworks and governance mechanisms to govern the deployment and operation of blockchain-based voting platforms, ensuring compliance with legal and regulatory requirements while fostering trust and confidence among stakeholders.

# REFERENCES

[1] Fakhar ul Hassan, Anwaar Ali, Siddique Latif, Junaid Qadir, Salil Kanhere, Jatinder Singh, and Jon Crowcroft.(2019) Blockchain And The Future of the Internet: A Comprehensive Review

[2] Simin Ghesmati, Walid Fdhila, Edgar Weippl (2023) User-Perceived Privacy in Blockchain

[3] Burcu Sakız, Aysen Hic Gencer (2019) Blockchain Technology and its Impact on the Global Economy

[4] B Laurie Hughes, Yogesh Kumar Dwivedi, Santosh K. Misra, Nripendra Rana (2019) Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda

[5] Satoshi Nakamoto (2009) Bitcoin: A Peer-to-Peer Electronic Cash System

[6] Merlinda An6doni, Valentin Robu, D. Flynn, Simone Abram (2018) Blockchain technology in the energy sector: A systematic review of challenges and opportunities

[7] Diego Moussallem, Matthias, Axel-Cyrille Ngonga Ngomo (2017) Machine Translation Using Semantic Web Technologies: A Survey

[8] Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends

[9] Gustavo Ansaldi Oliva, Ahmed E. Hassan, Zhen Ming (Jack) Jiang (2020) An Exploratory Study of Smart Contracts in the Ethereum Blockchain Platform

[10] Peter D. DeVries (2016) An Analysis of Cryptocurrency, Bitcoin, and the Future

[11] Van Giang Phan Mai, Lã Minh Vũ, Đỗ Hoàng Sơn, and Nguyễn Tuấn Khải (2023) A Blockchain-based User Authentication Model Using MetaMask

[12] Laiphrakpam Dolendro Singh, Khumanthem Manglem Singh (2015) Implementation of Text Encryption using Elliptic Curve Cryptography

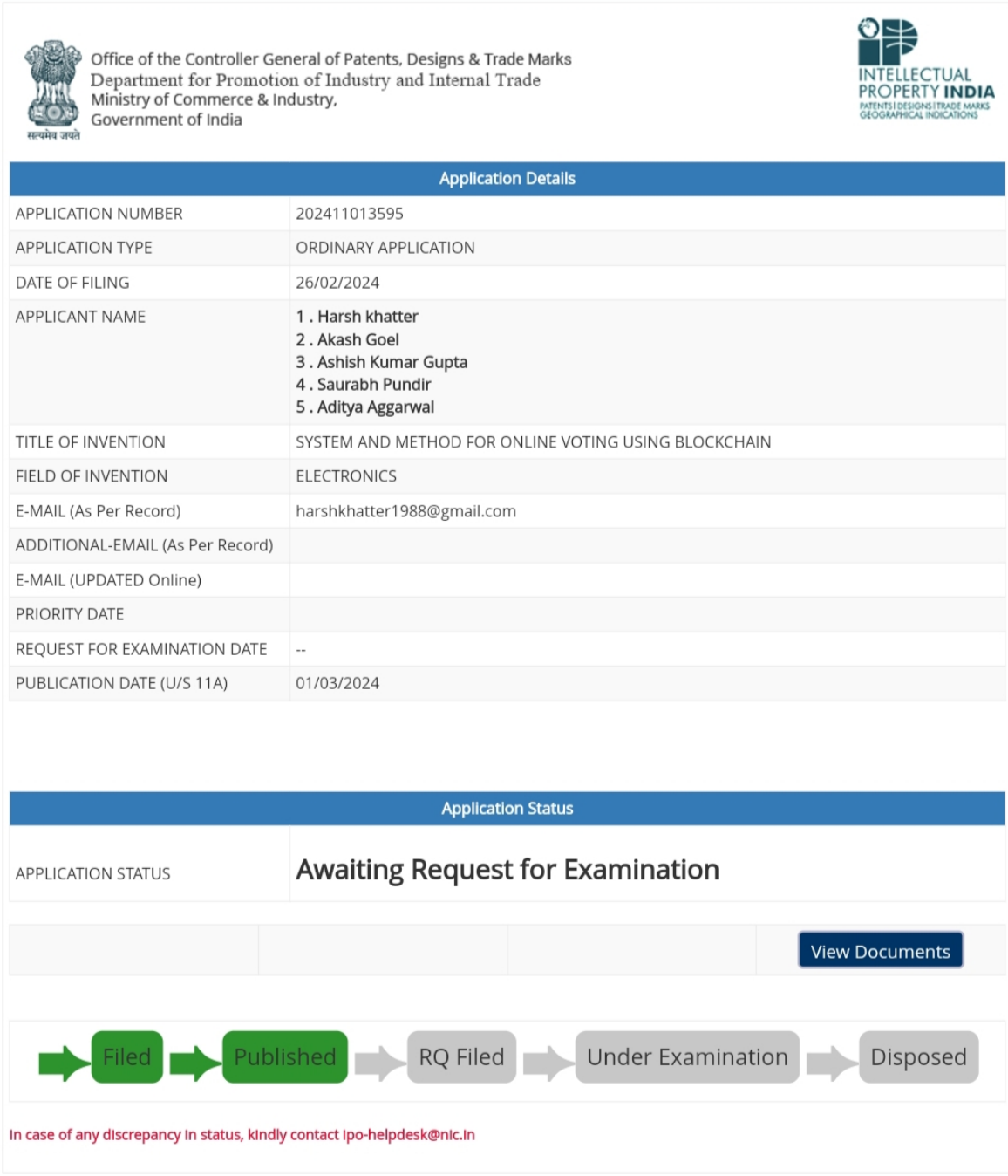
[13] Nwosu Anthony, S B Goyal, Anand Singh Rajawat, Sardar M. N. Islam (2022) An Innovative Blockchain-Based Secured Logistics Management Architecture: Utilizing an RSA Asymmetric Encryption Method

[14] Blockchain Technology Based Healthcare Supply Chain Management, Dr. Pushpa, International, Taylor & Francis Group, 978-1-003-20196- 0 (Book Chapter)

[15] Vikarnt Shokeen, Sachin Goel, Nidhi Gupta, Chhaya Sharma, Parita Jain, "Blockchain Technology and Its Industrial Utilization: A Review", DE, pp. 14570-14579, Sep. 2021

**GitHub Link:** https://github.com/t2geg/voting-dapp

# Proof of patent publication



Office of the Controller General of Patents, Designs & Trade Marks
Department for Promotion of Industry and Internal Trade
Ministry of Commerce & Industry,
Government of India

INTELLECTUAL PROPERTY INDIA
PATENTS | DESIGNS | TRADE MARKS
GEOGRAPHICAL INDICATIONS

| Application Details | |
|---|---|
| APPLICATION NUMBER | 202411013595 |
| APPLICATION TYPE | ORDINARY APPLICATION |
| DATE OF FILING | 26/02/2024 |
| APPLICANT NAME | 1 . Harsh khatter<br>2 . Akash Goel<br>3 . Ashish Kumar Gupta<br>4 . Saurabh Pundir<br>5 . Aditya Aggarwal |
| TITLE OF INVENTION | SYSTEM AND METHOD FOR ONLINE VOTING USING BLOCKCHAIN |
| FIELD OF INVENTION | ELECTRONICS |
| E-MAIL (As Per Record) | harshkhatter1988@gmail.com |
| ADDITIONAL-EMAIL (As Per Record) | |
| E-MAIL (UPDATED Online) | |
| PRIORITY DATE | |
| REQUEST FOR EXAMINATION DATE | -- |
| PUBLICATION DATE (U/S 11A) | 01/03/2024 |

| Application Status | |
|---|---|
| APPLICATION STATUS | Awaiting Request for Examination |

View Documents

Filed → Published → RQ Filed → Under Examination → Disposed

In case of any discrepancy in status, kindly contact ipo-helpdesk@nic.in