# Z VOTE-BLOCKCHAIN BASED E-VOTING SYSTEM

MINIPROJECT REPORT

submitted by

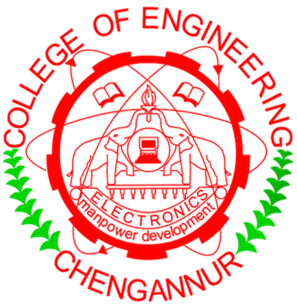
**AKASH S(CHN20CS012)**

to

*APJ Abdul Kalam Technological University*

*in partial fulfillment of the requirements for the award of B.Tech Degree in*

*Computer Science & Engineering*




**DEPARTMENT OF COMPUTER ENGINEERING**

**COLLEGE OF ENGINEERING CHENGANNUR, ALAPPUZHA**

**JULY 2023**

# DECLARATION

I undersigned hereby declare that the project report "**Z Vote-Blockchain based e-voting system**" , submitted for partial fulfillment of the requirements for the award of degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of **Smt. Shemeema Hashim**.This submission represents my ideas in my own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

**Place:** Chengannur

**Date :** 04/07/2023

**Akash S**

**DEPARTMENT OF COMPUTER ENGINEERING**

**COLLEGE OF ENGINEERING CHENGANNUR**

**ALAPPUZHA**

## CERTIFICATE

*This is to certify that, the project report titled* ***Z VOTE-BLOCKCHAIN BASED E-VOTING SYSTEM*** *by* ***AKASH S****(CHN20CS012), to* ***APJ Abdul Kalam Technological University***. in partial fulfillment of the **B. Tech. Computer Science and Engineering** is a bonafide record of the project work carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

| | | |
|---|---|---|
| **Smt. Shemeema Hashim** | **Smt. Syeatha Merlin Thampy** | **Dr. Manju S Nair** |
| Guide | Project Coordinator | Head of the Dept. |
| Assistant Professor | Assistant Professor | Associate Professor |
| Dept.of Computer Engineering | Dept.of Computer Engineering | Dept.of Computer Engineering |

# ACKNOWLEDGEMENT

This work would not have been possible without the support of many people. First and foremost, I give thanks to Almighty God who gave me the inner strength, resources, and ability to complete my project successfully.

I would like to thank **Dr. Smitha Dharan**, The Principal, who has provided me with the best facilities and atmosphere for the project completion and presentation. I would also like to thank HOD **Dr. Manju S Nair** (Associate Professor, Computer Engineering), my project coordinator **Smt. Syeatha Merlin Thampy** (Assistant Professor, Computer Engineering), my project guide **Smt. Shemeema Hashim** (Assistant Professor, Computer Engineering) for the extended help and the encouragement and support given to me while doing the project.

I would like to thank our dear friends and faculties for extending their cooperation and encouragement throughout the project work, without which I would never have completed the project this well. Thank you all for your love and also for being very understanding.

**Akash S**

# ABSTRACT

Blockchain technology has gained significant attention in recent years due to its potential to revolutionize various industries. One such industry that can benefit greatly from blockchain is the voting system. Traditional voting systems are often plagued with challenges such as security vulnerabilities, lack of transparency, and potential for manipulation. In this context, a blockchain-based e-voting system offers a promising solution to address these issues and enhance the integrity and efficiency of the voting process. This project presents an abstract for a blockchain-based e-voting system that leverages the decentralized and immutable nature of blockchain technology. The proposed system employs cryptographic algorithms to ensure secure and verifiable transactions, making it nearly impossible for unauthorized individuals to tamper with the voting data. By storing votes on a distributed ledger, the system enhances transparency and allows all stakeholders to independently verify the authenticity of the results. To enhance accessibility and convenience, the proposed system incorporates user-friendly interfaces, enabling voters to cast their ballots securely from anywhere with an internet connection. Furthermore, the system provides real-time monitoring and auditing capabilities to authorized entities, allowing them to ensure the integrity and fairness of the voting process. Through the use of blockchain technology, this e-voting system offers numerous advantages, including enhanced security, transparency, immutability, and efficiency. While challenges such as scalability, identity verification, and voter trust remain, the potential benefits outweigh the obstacles. Future research and development efforts should focus on addressing these challenges and conducting large-scale pilot projects to validate the feasibility and effectiveness of blockchain-based e-voting systems.

# CONTENTS

# LIST OF FIGURES

# CHAPTER 1

# INTRODUCTION

## 1.1 Project Area

The integrity and transparency of the voting process are fundamental pillars of any democratic society. However, traditional voting systems often face various challenges, including security vulnerabilities, potential for fraud, lack of transparency, and logistical inefficiencies. In recent years, blockchain technology has emerged as a promising solution to address these issues and revolutionize the way we conduct elections. By leveraging the decentralized and immutable nature of blockchain, a blockchain-based e-voting system offers the potential to enhance the security, transparency, and efficiency of the voting process.

Blockchain, originally introduced as the underlying technology for cryptocurrencies like Bitcoin, is a distributed ledger that enables secure and transparent record-keeping of transactions. It operates on a network of decentralized nodes, where each node maintains a copy of the entire blockchain, ensuring consensus and eliminating the need for a central authority. The immutability of blockchain, achieved through cryptographic hashing and consensus mechanisms, makes it extremely difficult for any party to tamper with the data stored on the blockchain.

Here are some key features and benefits of blockchain based e-voting system are Blockchain Technology: Understanding and implementing the fundamentals of blockchain technology, including decentralized consensus mechanisms, cryptographic hashing, smart contracts, and blockchain data structures.Security and Privacy: Addressing the security challenges involved in electronic voting, such as protecting against unauthorized access, tampering, and ensuring voter anonymity while maintaining the integrity of the voting process.Voter Authentication: Designing a robust system for voter authentication to prevent fraudulent voting and ensure that only eligible voters can cast their ballots.User Interface and Experience: Developing an intuitive and user-friendly interface for voters to participate in the e-voting process easily.Scalability: Addressing the scalability challenges of blockchain to handle a large number of voters and votes without compromising on performance.Post-election Auditing and Transparency: Designing mechanisms for post-election

auditing and providing transparent access to voting records for verification.Accessibility and Inclusivity: Ensuring the e-voting platform is accessible to all eligible voters, including those with disabilities.Partnerships and Collaboration: Collaborating with relevant authorities, election commissions, and stakeholders to gain support and facilitate the adoption of the e-voting system.Public Perception and Trust: Addressing concerns related to public perception and building trust in the security and accuracy of the e-voting system.

## 1.2 Objectives

- Utilize the transparent and immutable nature of blockchain to ensure that all cast votes are recorded in a tamper-proof manner.
- Employ cryptographic techniques and consensus algorithms to safeguard the voting data from unauthorized access, tampering, or manipulation.
- Implement a robust voter authentication system to verify the eligibility of each voter, ensuring that only authorized individuals can cast their votes.
- Ensure voter anonymity by separating the voter's identity from their vote. This protects voter's privacy and prevents coercion or vote-buying.
- Use blockchain's distributed ledger to prevent double voting and ensure that each voter can cast only one vote.
- Increase accessibility for voters, including those with disabilities, by providing a user-friendly electronic platform for voting from anywhere with an internet connection.

# CHAPTER 2

# LITERATURE SURVEY

## 2.1 Blockchain Enabled E-Voting by Nir Kshetri, Jeffry Voas

In this paper [1], eligible voters cast a ballot anonymously using a computer or smartphone. BEV employs an encrypted key and tamperproof personal IDs. For example, the mobile e-voting platform of the Boston-based startup Voatz employs smart biometrics and real-time ID verification. The public ledger ties each cast ballot to an individual voter and establishes a permanent, immutable record. No bad actor can engage in nefarious activities because such activities will be evident on the ledger or corrected by a peer-to-peer consensus network.

To compromise the network, hackers would need to successfully hack most of the blocks (files with transaction records) before new blocks were introduced. The blockchain's audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added. Put simply, blockchains enable the creation of tamper-proof audit trails for voting. In this article, we highlight some BEV implementations and the approach's potential benefits and challenges.

Each voter is considered as a wallet, and the transactions between wallet is limited to one. As the candidates are considered as the receiver wallet. The vote is actually the transaction between all the candidates or receiver wallets. The methodology used in this paper is Blockchain enabled e-voting which is using an encrypted key along with the alteration-proof user IDs. The advantage is Blockchain enabled e-voting will help us to ensure the aspect of security as well as transparency which would help to reduce electoral violence and produce more mathematically precise voting results.

The Disadvantage is They did not use a decentralized voting system (only meant for one single place). No consensus. The wallet-coin model can be amended to single wallet

## 2.2 Blockchain-Based E-Voting System by Fririk . Hjálmarsson, Gunnlaugur K. Hreiarsson, Mohammad Hamdaqa, Gísli Hjálmtýsson

This paper[2] attempts to use a case study to determine the potential of distributed ledger technologies, such as the election process and its implementation via a blockchain-based framework, which will boost security and reduce the cost of conducting national elections. The technique is to achieve these objectives by using a Go-Ethereum Proof-of-Authority (POA) blockchain authorization setup They have used the algorithm through a process based on identity as a stake, which delivers faster transactions. They use district and boot. The voting data is checked by the majority of the district nodes when any individual elector casts a vote from their compliant smart contract, and any vote they agree on is appended to the blockchain. The advantage is Elections can be used as a Blockchain part of Smart Contract, using developer friendly Framework (Go-Ethereum), Centralized consensus.

The blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some additional measures would be needed to support greater throughput of transactions per second.

The disadvantage is limited up to 5000 votes/second. Can use some better blockchain frameworks for increasing transactions per second.

## 2.3 A Blockchain-Based Network Security Mechanism for Voting Systems by Hsin-Te Wu, Chang-Yi Yang

This paper[3] proposes a local voting mechanism conceptualized on block-chain to help decision making for its peers' networks. It protects the privacy and enables detection as well as correction against cheating. The methodology used are Distributed consensus based blockchain algorithm. The advantage is Elections can be used as a Blockchain part of Smart Contract, Peer to peer network, consensus, Two phase validation (decryption pvt key, smart contract verification).

This study utilizes bilinear pairing to establish network security in voting systems, which call for anonymity, authenticity, integrity, and non-repudiation. When authenticating voting integrity, the

user's anonymity must be ensured to prevent identity revelation, and the data must be protected against malicious tampering such security measures also fulfill blockchain requirements. The proposed voting system relies on the basis of blockchains to create a trustworthy voting system.
In current blockchain technology, smart contracts allow the establishment of voter related regulations to prevent controversies during voting processes. Additionally, in order to establish both a secret ballot and an open ballot system, the study also implements a bilinear pairing security mechanism to ensure the overall security of a voting procedure.
The disadvantage is there is no proof if the model will work or not. Untested with many blockchain frameworks. Can use a better blockchain framework for increasing transactions per second. If tested with faster and premised blockchain frameworks it can set the standards.

## 2.4 Trustworthy Electronic Voting Using Adjusted Blockchain Technology by Basit Shahzad, Jon Crowcroft

This paper[4] suggests a framework by using effective hashing techniques to ensure the security of the data. The concept of block creation and block sealing is introduced in this paper. The introduction of a block sealing concept helps in making the blockchain adjustable to meet the need of the polling process. The use of consortium blockchain is suggested, which ensures that the blockchain is owned by a governing body (e.g., election commission), and no unauthorized access can be made from outside.
The framework proposed in this paper discusses the effectiveness of the polling process, hashing algorithms' utility, block creation and sealing, data accumulation, and result declaration.
To ensure data protection, such as block formation and sealing, it proposes useful hashing techniques. The methodology used are consensus based blockchain algorithm. The advantages are Used their own framework, Better hashing algorithm.
The disadvantage is there is no proof if the model will work or not, Untested with many blockchain frameworks.

## 2.5 DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system by Syada Alvi, Mohammed Uddin, Linta Islam, Sajib Ahamed

In this paper[5] used blockchain technology anonymity, privacy, verifiability, mobility, integrity, security, and fairness in voting. By using blockchain our proposed system ensures security, privacy,

and integrity. This system provides voter anonymity by keeping the voter information as a hash in the blockchain. It also provides fairness by keeping the casted vote encrypted till the ending time of the election. After ending time, the voter can verify their casted vote, ensuring verifiability. To test this protocol, they put it on Ethereum 2.0, a blockchain platform that uses Solidity as a programming language to create smart contracts. The adoption of smart contracts provides a safe means for performing voter verification, ensuring the correctness of voting results, making the counting system public, and protecting against fraudulent activities. They analyzed the system's performance based on security and gas costs. It improves in terms of security characteristics and the related cost for the necessary infrastructure.

The limitation of this system is that they did not implement the OTP (One Time Password) option in registration process. Another limitation is that they have stored the encrypted vote in the blockchain during vote casting. This data will not be used after the end of the election. For storing these data, the cost has increased.

## 2.6 A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems by Uzma Jafar,Mohd Juzaiddin Ab Aziz,Zarina Shukur and Hafiz Adnan Hussain

This paper[6] seeks to highlight the solutions regarding scalable Blockchain-based electronic voting systems and the issues linked with them while also attempting to foresee future developments. A systematic literature review (SLR) was used to complete the task, leading to the selection of 76 articles in the English language from 1 January 2017 to 31 March 2022 from the famous databases. This SLR was conducted to identify well-known proposals, their implementations, verification methods, various cryptographic solutions in previous research to evaluate cost and time. It also identifies performance parameters, the primary advantages and obstacles presented by different systems, and the most common approaches for Blockchain scalability. In addition, it outlines several possible research avenues for developing a scalable electronic voting system based on Blockchain technology.

## 2.7 Gap Identified

We have identified that the current system does not have the OTP option in the registration process, which increases the chance of tampering,our proposal aims to implement an OTP verification which is fully decentralised and web based enabling maximum participation in the voting process. Thus concluding by emphasizing the potential of this system to transform the way we conduct elections.

# CHAPTER 3

# PROBLEM DEFINITION

## 3.1 Problem Statement

To develop a decentralized blockchain-based e-voting system that provides secure voter authentication, anonymized voting, tamper-proof storage of ballots, and transparent verification of election results to address the shortcomings of traditional voting methods.

## 3.2 Existing System

Voters need to go personally to a polling booth to cast their vote, which includes several identification steps. Implementation of work force, and other machineries cause excess cost. Lot of time is wasted during these processes. It does not allow the voters to review and audit vote they casted.

## 3.3 Limitations

- Security Vulnerabilities: Electronic voting systems can be susceptible to hacking, cyberattacks, and tampering.
- Lack of Voter Verification: Some voting systems may not have robust mechanisms for verifying voter identity.
- Limited Accessibility: Not all voting systems are accessible to individuals with disabilities, which can disenfranchise a significant portion of the population.
- Voter Disenfranchisement: Issues with voter registration, strict identification requirements, or limited polling locations can lead to voter disenfranchisement and reduced voter turnout.
- Privacy Concerns: Some electronic voting systems may not adequately protect voter privacy.
- Transparency and Auditing: Certain voting systems lack transparency, making it difficult for independent audits to verify the accuracy and legitimacy of election results.
- Lack of Standardization: Different regions or countries may use disparate voting systems, making it difficult to compare and evaluate election practices.
- Costs: Implementing and maintaining voting systems, especially electronic ones, can be costly, and the financial burden may limit the adoption of more advanced technologies.

## 3.4 Proposed Model

This e-voting system is user-friendly and intuitive, with a simple and elegant interface that allows voters to easily cast their vote from their computer or mobile device. The system has been designed with security and privacy in mind, and we have implemented a range of measures to protect the personal information of voters and prevent any attempts to hack the system.By leveraging the decentralized and immutable nature of blockchain technology, the project aims to significantly enhance the security of the e-voting system. The use of cryptographic algorithms ensures the integrity of transactions and makes it extremely difficult for unauthorized individuals to tamper with voting data. Introduces a transparent and auditable voting process. By storing votes on a public blockchain, the entire process becomes transparent.Individual votes are encrypted and anonymized, protecting the identity of voters while allowing for auditing of the overall system integrity. We uses One-Time Passwords (OTP) verification. OTPs are time-limited and can only be used once, reducing the risk of unauthorized access even if the password is intercepted. Through the introduction of a blockchain-based e-voting system, the project contributes to building trust among stakeholders, including voters, election officials, and regulatory bodies. By addressing security concerns, ensuring transparency, and providing verifiable results, the project aims to foster confidence in the integrity of the voting process.

# CHAPTER 4

# SYSTEM REQUIREMENT SPECIFICATION

## 4.1 Introduction

The 'Blockchain-based e-Voting System' is a cutting-edge electronic voting platform that aims to transform traditional voting methodologies by harnessing the potential of blockchain technology. This innovative system seeks to address the limitations of existing voting mechanisms, such as security vulnerabilities, lack of transparency, and concerns over data integrity. By utilizing blockchain's decentralized, tamper-resistant, and transparent nature, the proposed e-voting system strives to instill trust and confidence in the electoral process, empowering citizens to participate in a secure and efficient manner.

## 4.2 Functional Requirements

A blockchain-based voting system can have various functional requirements to ensure transparency, security, and efficiency. Here are some essential functional requirements for a blockchain-based voting system: Authentication and Identity Verification: The system should authenticate voters and verify their identities to ensure that only eligible individuals can participate in the voting process. This can be achieved through various means such as digital signatures, biometrics, or unique cryptographic identifiers. Ballot Creation and Distribution: The system should facilitate the creation and distribution of digital ballots to eligible voters. Each ballot should be unique, tamper-proof, and securely delivered to the intended recipient. Privacy and Anonymity: The system should ensure the privacy and anonymity of voters' choices, preventing any correlation between a voter's identity and their vote. Vote Casting and Verification: The system should enable voters to cast their votes securely and ensure that the votes are accurately recorded on the blockchain. It should provide mechanisms for voters to verify that their votes have been correctly registered. Consensus Mechanism: The system should incorporate a consensus mechanism that ensures agreement among all participants on the validity and order of vote transactions. This mechanism can be based on proof-of-work (PoW), proof-of-stake (PoS), or other consensus algorithms

## 4.3 Interface Reqirements

User Interface for the project was built using HTML. It is the primary language for building web pages and applications. Django Web Framework is core web framework, handling the server-side. It manages the routing, authentication, database interactions, and other backend functionalities. In Django, Gunicorn (short for Green Unicorn) is a commonly used web server that serves Django applications. Gunicorn is designed to be a lightweight, reliable, and efficient server that can handle high traffic loads. Nginx is used for the working of web server, NGINX is a popular open-source web server and reverse proxy server known for its high performance, scalability, and efficient handling of concurrent connections. It is widely used as a front-end web server to serve static and dynamic content and also as a load balancer to distribute incoming requests across multiple servers. we use symmetric and asymmetric encryption for advanced security of votes. The hardware requirements include the requirements specification of the physical computer resources for a system to work efficiently. The hardware requirements may serve as the basis for a contract for the implementation of the system and should therefore be a complete and consistent specification of the whole system. The Hardware Requirements for the proposed system include Intel/AMD - 2 GHz or faster processor, 32-bit or 64-bit Architecture, 1 GB RAM and 1 GB Hard disk . The software requirements are description of features and functionalities of the target system. Requirements convey the expectations of users from the software product. The requirements can be obvious or hidden, known or unknown, expected or unexpected from client's point of view. The Hardware Requirements for the proposed system is the Operating System: Linux-for better server compatibility.

## 4.4 Performance Requirements

Performance requirements define how well the software system accomplishes certain functions under specific conditions. Examples include the software's speed of response, throughput, execution time and storage capacity. The service levels comprising performance requirements are often based on supporting end-user tasks. Throughput: The system should be capable of handling a high number of transactions or votes per second. This includes the ability to process and record votes on the blockchain in a timely manner to prevent delays and ensure a smooth voting experience. Latency: The system should minimize the time between vote submission and its inclusion in the blockchain. Low latency is crucial to provide real-time feedback to voters, allowing them to verify the acceptance of their votes and ensuring a seamless and responsive voting process. Scalability: The e-voting system should be designed to handle an increasing number of voters and votes without compromising its performance. As the number of participants grows, the system should be

able to scale horizontally or vertically to accommodate the increased demand without significant degradation in speed or responsiveness. Network Efficiency: The efficiency of the network used by the e-voting system is crucial to ensure quick dissemination of information across the blockchain network. The system should optimize network utilization, minimize bandwidth requirements, and reduce network congestion to maintain optimal performance. Computational Efficiency: The computational demands of the e-voting system should be optimized to minimize resource requirements, such as processing power and memory usage. Efficient algorithms and data structures should be employed to reduce the computational complexity and enhance overall system performance.

## 4.5 Non Functional Requirements

Measures are made so that system provide better accuracy, have simple interface for users to use and perform efficiently in less amount of time.

Security: The system must ensure the confidentiality, integrity, and availability of all data, including user information and voting records. The system must implement strong authentication and authorization mechanisms to prevent unauthorized access. The system must use blockchain technology to ensure transparency, immutability, and tamper-proof records of all votes and activities.

Performance: The system must be able to handle plenty of concurrent users and votes during peak times without any performance degradation. The system must have low latency and high throughput for vote processing and result generation.

Usability: The system must have a user-friendly and intuitive interface for both admin users and voters. The system must provide clear instructions and guidance to users throughout the voting process.

Reliability: The system must be highly reliable and available 24/7 to ensure continuous and uninterrupted voting process. The system must have backup and recovery mechanisms in place to handle any data loss or system failures.

# CHAPTER 5

# PROJECT DESIGN

## 5.1 System Architecture Design

The system architecture design of a web-based e-voting system based on blockchain, built using the Django framework, Bootstrap, MySQL, and HTML, involves several components working together to provide a secure and reliable e-voting experience.

- User Interface (UI) layer encompasses the client-side components responsible for presenting the user interface and handling voter interactions. It includes the web interface developed using HTML,Bootstrap.
- Authentication is controlled by functions in the Django framework.
- For structured data like voter information and vote information ,candidate information MySQL database is used

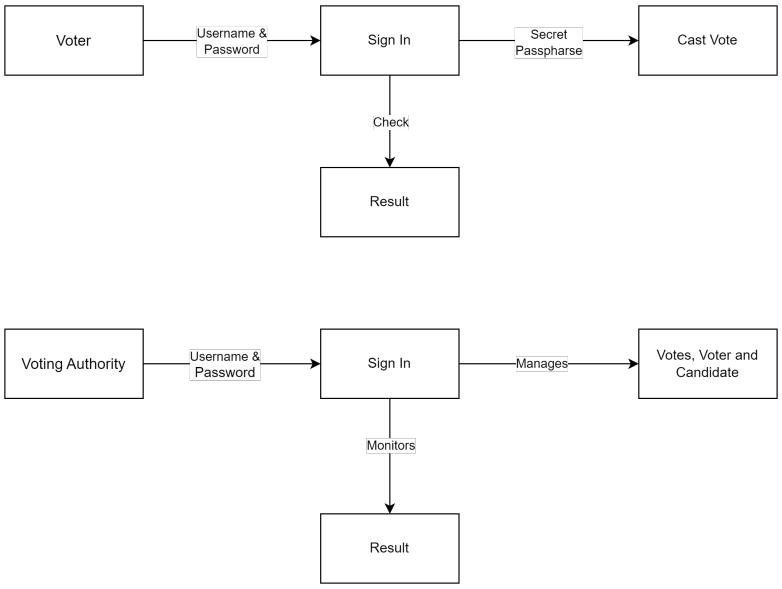



Figure 5.1: Basic System Architecture

## 5.2 Application Architecture Design

Client-Side Components:

Web Browser: Users interact with the e-voting system through a web browser, which renders the user interface (HTML templates) and handles user input.

HTML and Bootstrap: The user interface is designed using HTML templates, which structure the content and presentation of the web pages. Bootstrap CSS framework can be used to enhance the UI design and responsiveness.

Web Server:

Django Web Framework: Django acts as the web framework, the entire backend works on this framework

Django Views: All working functions of our voting system comes under django views.Views perform data validation, and interact with other components to generate appropriate responses.

Django Models: Models define the structure of all database in the e-voting system.

Django Templates: Stores all the web pages to be provided.

Database Layer:

MySQL Database: MySQL is used to store and retrieve various data related to the e-voting system, including user profiles, election configurations, candidate information, and vote records.

BlockChain: Uses an implementation model blockchain. merkle tree hashing is used to simulate the blockchain. A Merkle tree, also known as a hash tree, is a data structure used in cryptography.

Security Layer:

User Authentication: The e-voting system employs user authentication mechanisms, such as username/password or two-factor authentication.

Encryption: Sensitive data, such as voter information or voting records, can be encrypted to ensure confidentiality and protect against unauthorized access.

Auditing and Logging: The system can log important events and activities for auditing purposes, providing a traceable record of system operations.

Security Best Practices: Implementation of secure coding practices, input validation, secure communication (HTTPS), and protection against common web vulnerabilities.

External Systems Integration:

External APIs: The e-voting system uses external APIs for passphrase retravel and OTP sending

Result Tabulation Systems:The e-voting system integrates with result tabulation systems, reporting mechanisms, and various components to form a web-based e-voting solution.

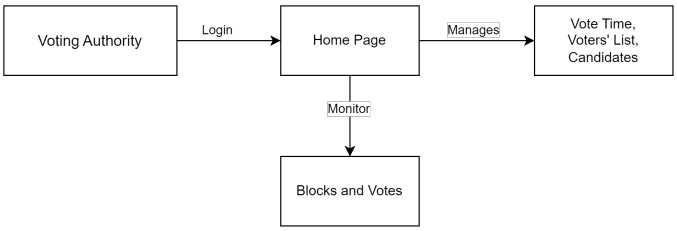



Figure 5.2: Voting Authority

Fig 5.2 shows the functions of voting authority,voting authority can login to home page and monitor blocks and votes along with the management of voting time,voters list .


Figure 5.3: Voters Registration

Fig 5.3 shows voter registration,after registration voter can validate OTP and set password and then using the secret passphrase can cast the vote

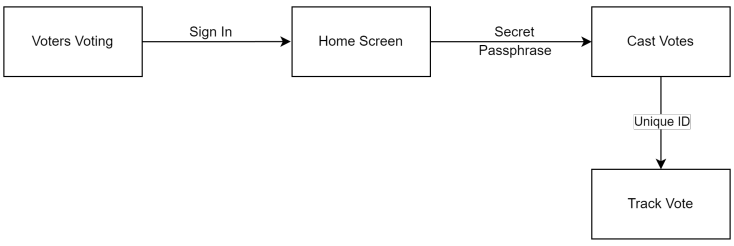



Figure 5.4: Voters Voting

Fig 5.4 Shows the voting process first voter has to sign in then using secret passphrase can cast vote.After voting we get a unique id with which we track our vote.

## 5.3 GUI Design

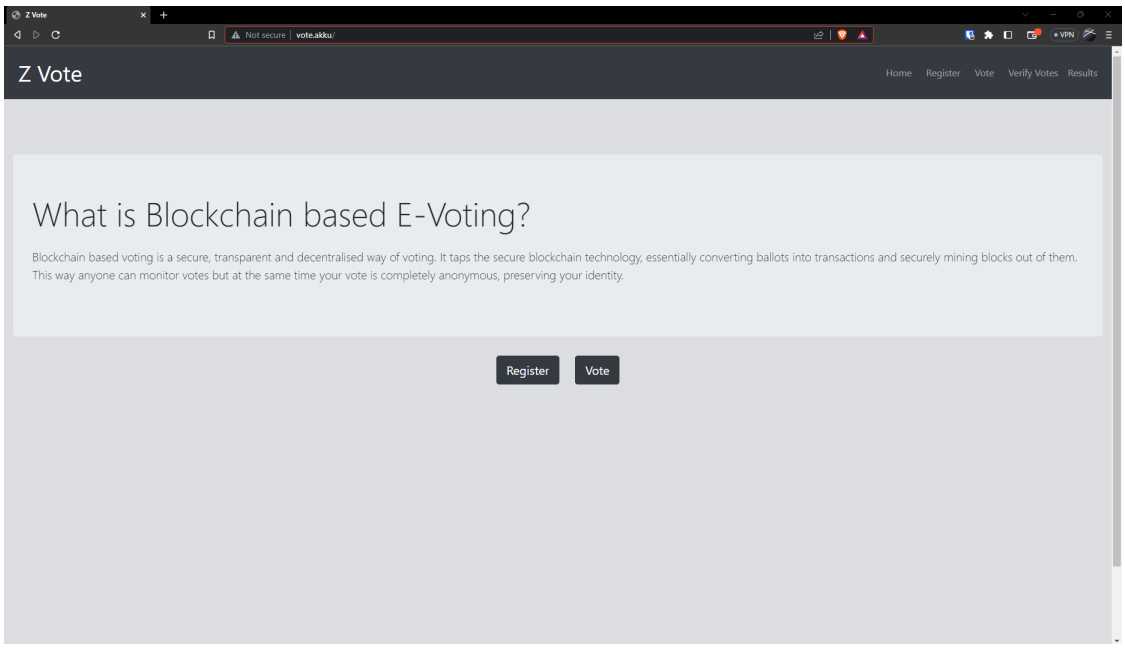



Figure 5.5: Home Page

On the home page (refer to Fig 5.5), users are presented with two prominently displayed buttons: ”Register” and ”Vote”.Only registered voters can vote

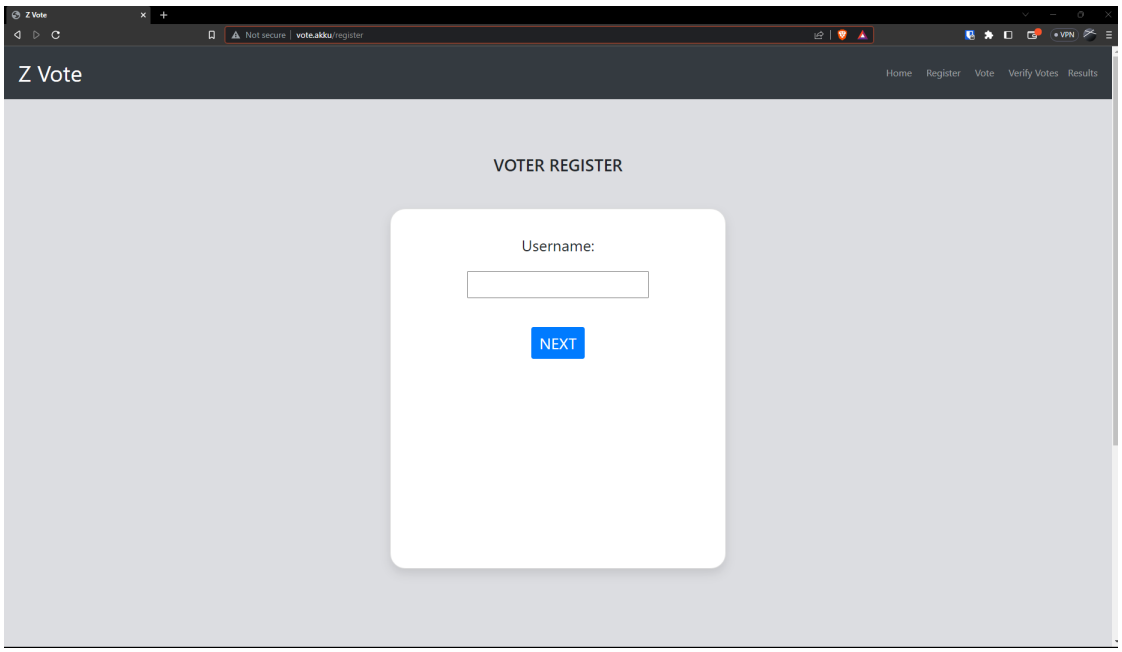



Figure 5.6: Register Page

Here in voter registration page (refer to Fig 5.6).users are prompted to enter their desired username, and upon completion, they can proceed to the next step by selecting the ”Next” button.

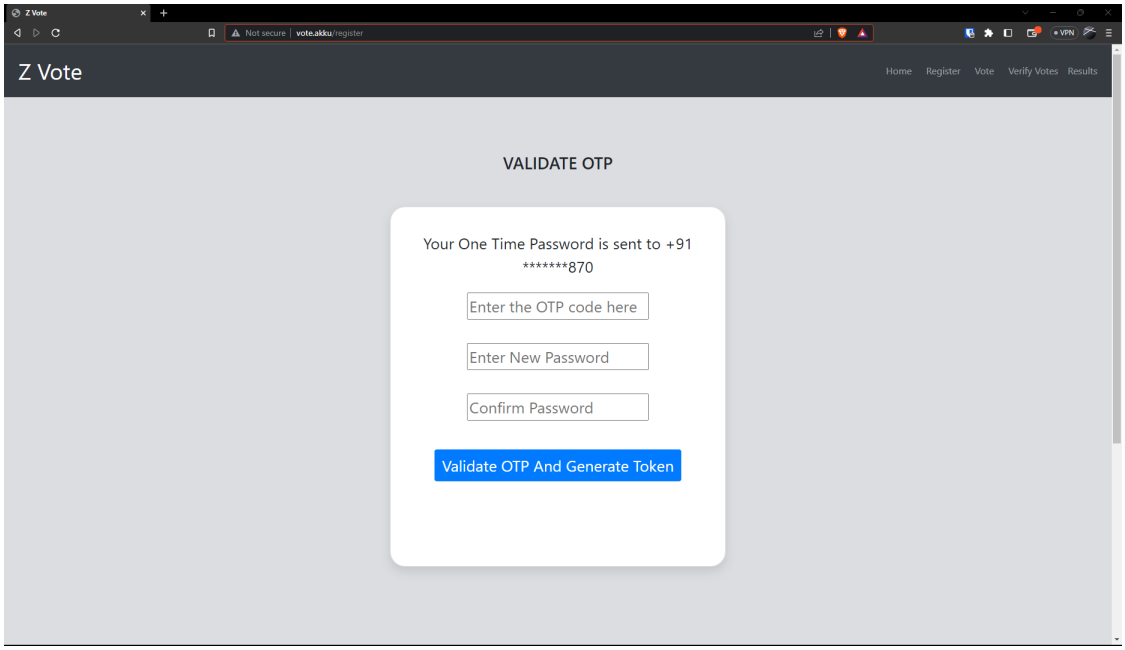



Figure 5.7: OTP page

Upon reaching the subsequent page (refer to Fig 5.7), the system initiates the verification process by validating the One-Time Password (OTP) that was sent to the voter’s registered phone number.

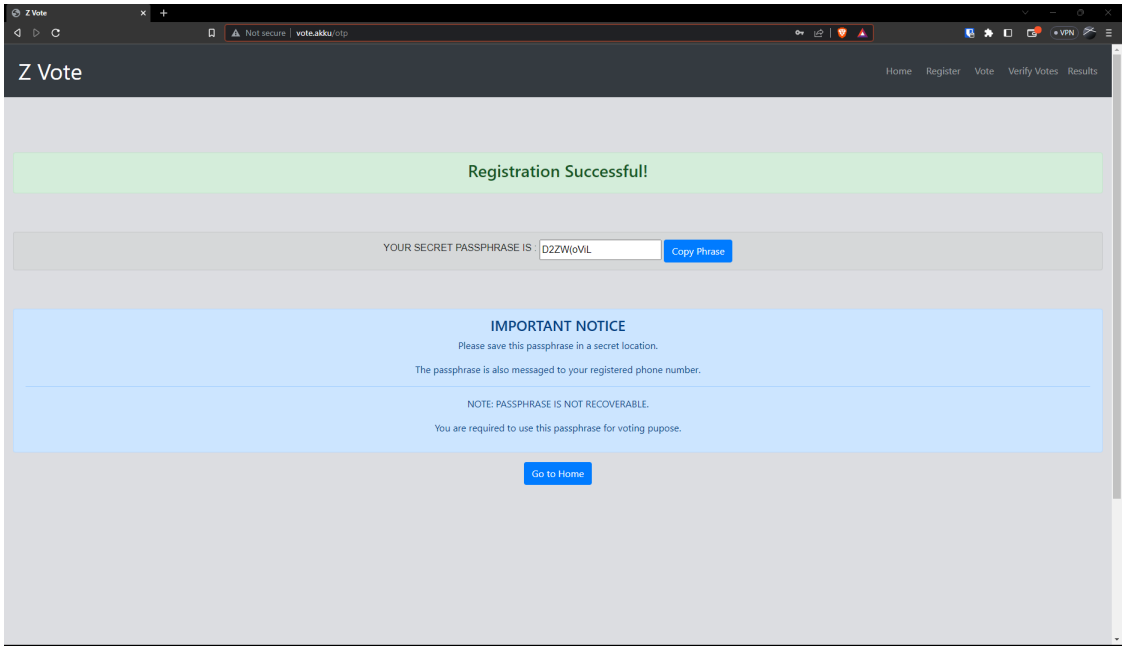



Figure 5.8: Registration successful page

This passphrase generated (refer to Fig 5.8) serves as a crucial key for the voting process, ensuring security and authenticity.The passphrase is transmitted to the voter's phone via a text message.

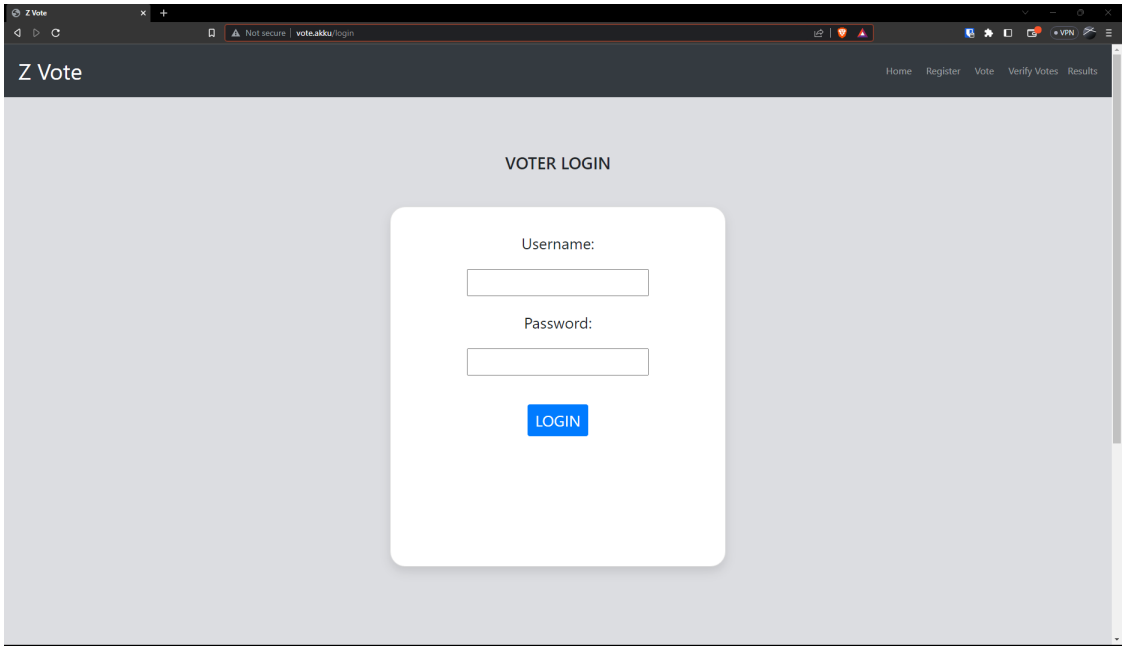



Figure 5.9: Login page

On this page(refer to Fig 5.9). the voter is required to enter their username and the password they previously set during the registration process. The voter can proceed by clicking the "Login" button.

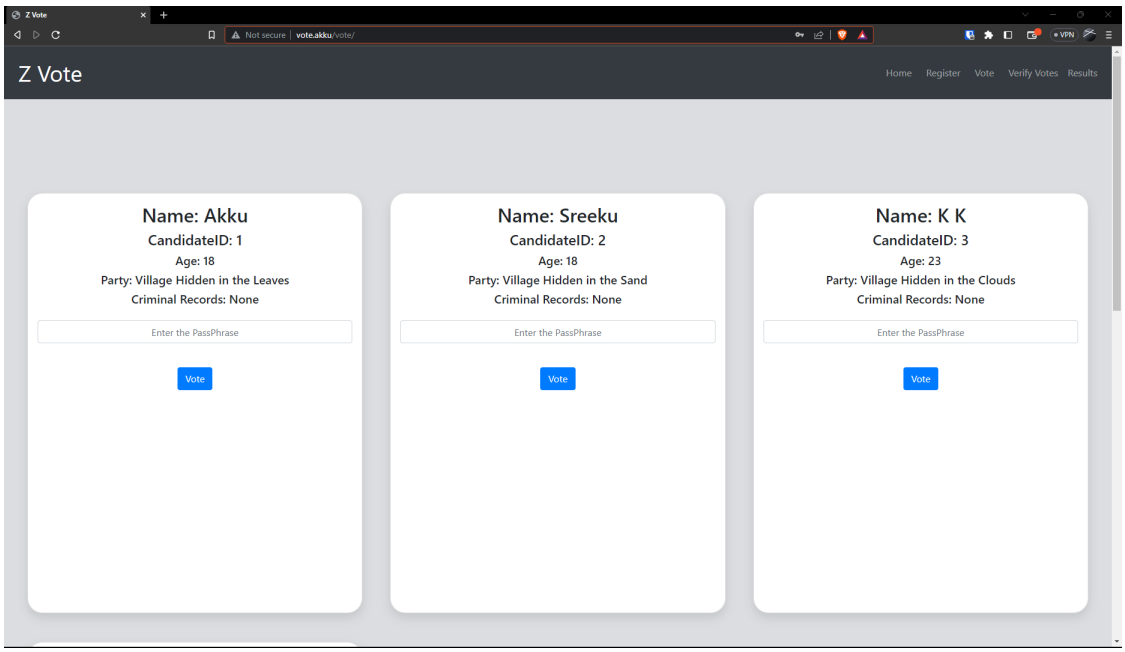



Figure 5.10: Voting page

Upon successful authentication, the voting page (refer to Fig 5.10) is displayed, presenting the voter with a list of candidates. To cast their vote the voter needs to enter the secret passphrase.

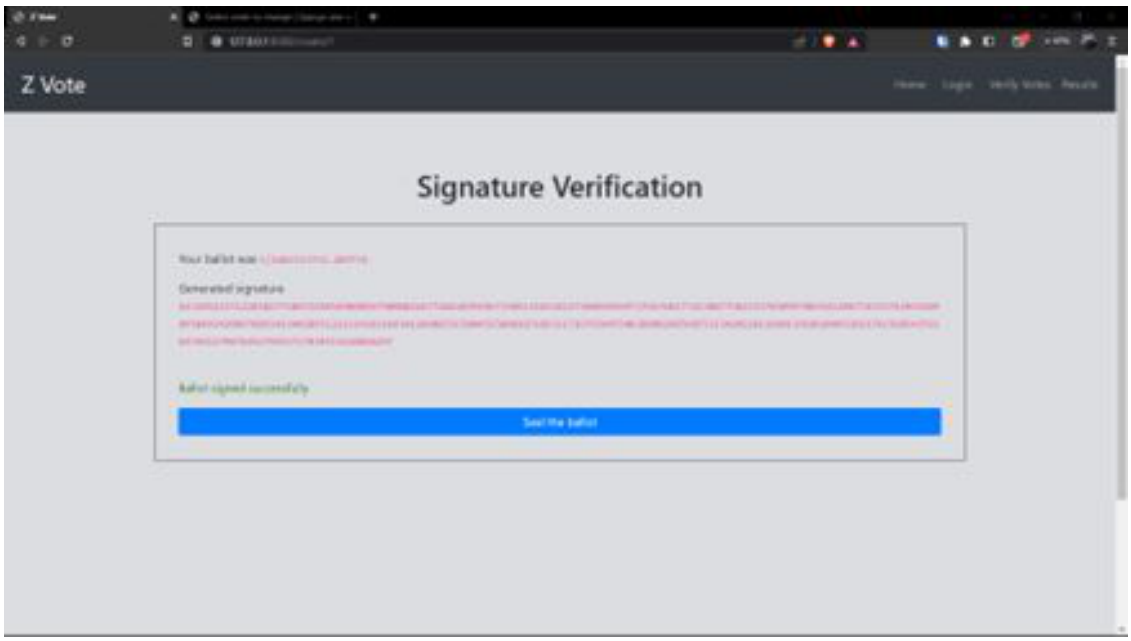



Figure 5.11: Ballot Verification

After casting vote in the voting page the voter is directed to the ballot verification page(refer to fig 5.11) where we can seal the ballot.By sealing the ballot your vote would be tamper proof.

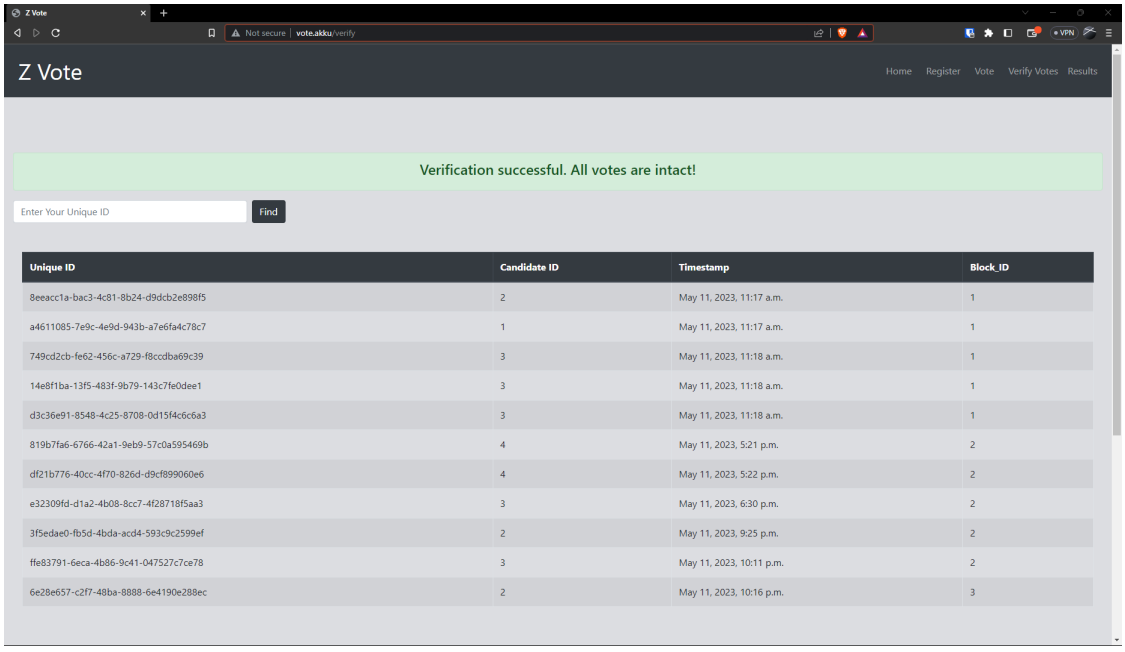



Figure 5.12: Vote Verification page

Clicking on the ”Verify Vote” button located in the top right corner of the page. This action leads them to a dedicated page (refer to Fig 5.12). On this page, the voter is prompted to enter their unique identification (ID), which serves as a means to authenticate their vote. Once the ID is entered, the voter can proceed by clicking the ”Find” button to initiate the verification process.

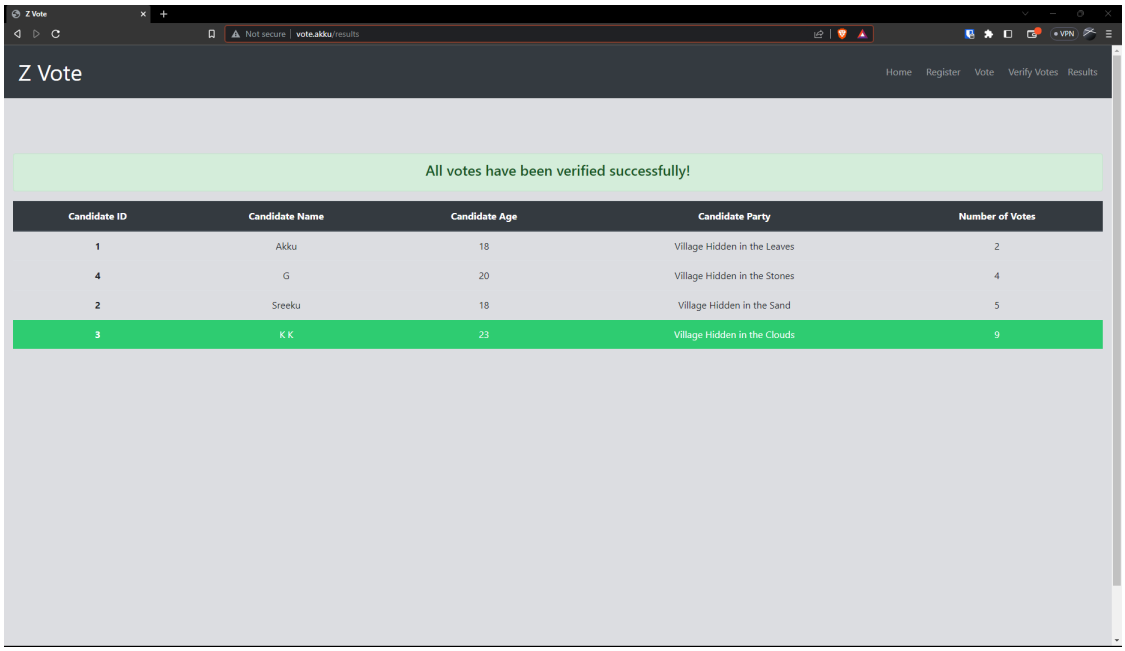



Figure 5.13: Result

Additionally, the voter has the ability to check the election results by clicking on the ”Results” button located in the top right corner. This action opens the Results page (refer to Fig 5.13), where the voter can view the outcome of the election. The winning candidate will be highlighted in a distinctive green color, making it easily identifiable. It is important to note that the results will only be accessible once the voting process has concluded.

## 5.4 API Design

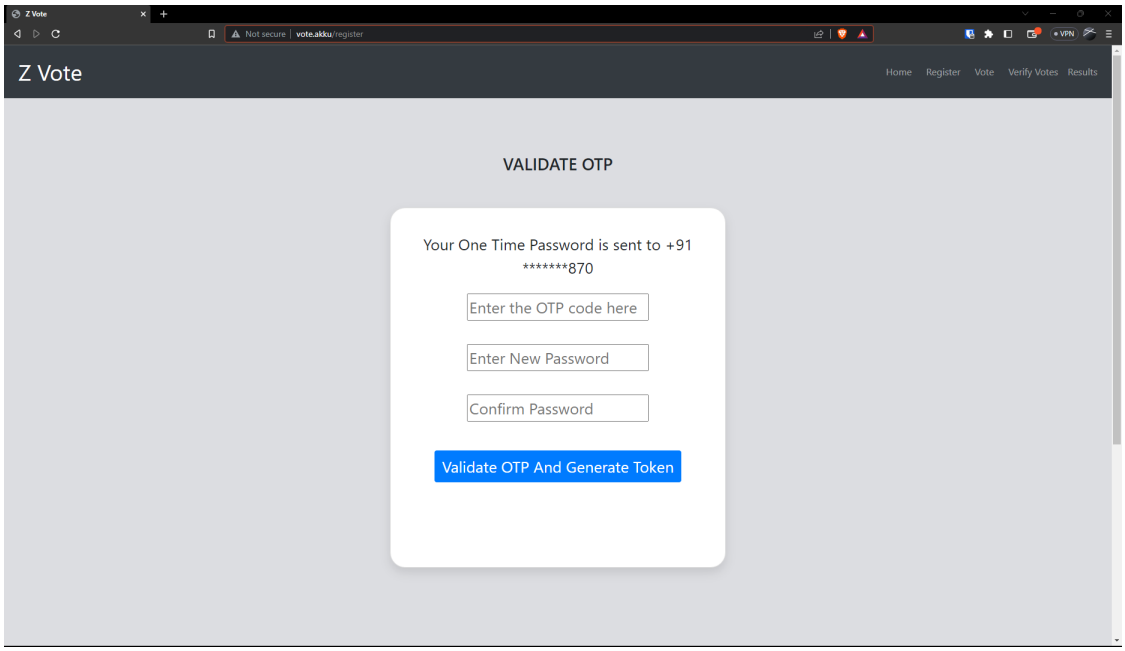



Figure 5.14: Validate OTP page

Validate OTP page(refer ti Fig 5.14) is used for OTP verification and password generation. The registered phone number of the voters and voters identity is verified in this stage

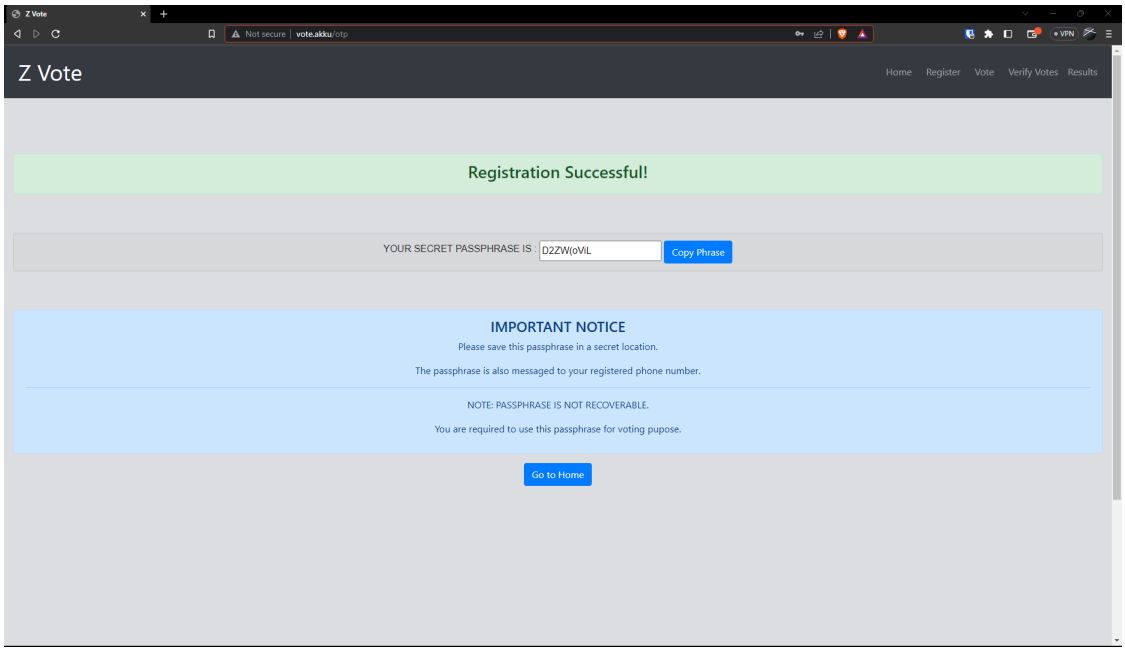



Figure 5.15: Registration successful page

Register successful page(refer to Fig 5.15)is shown when the registration of a voter is completed.This page provides a secret passphrase to the voter to vote.

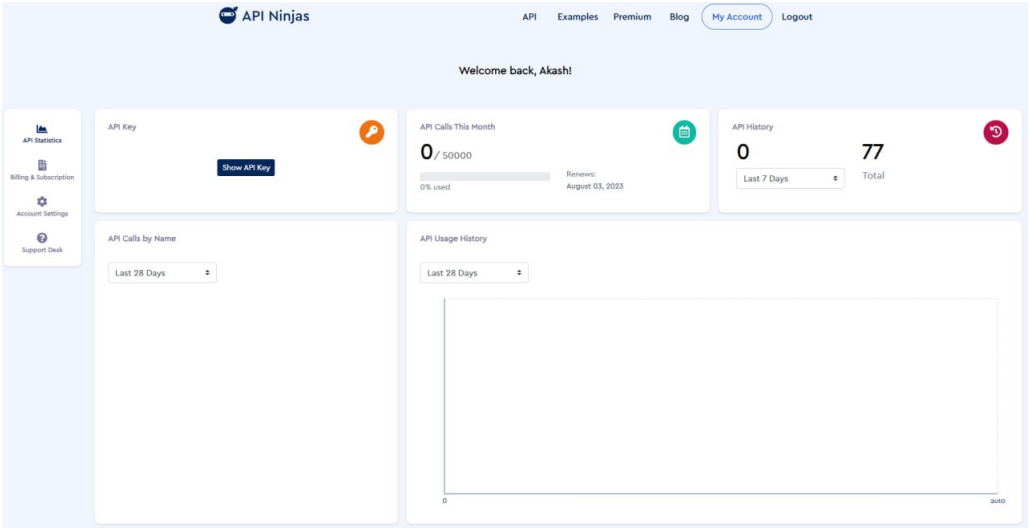



Figure 5.16: API Ninjas

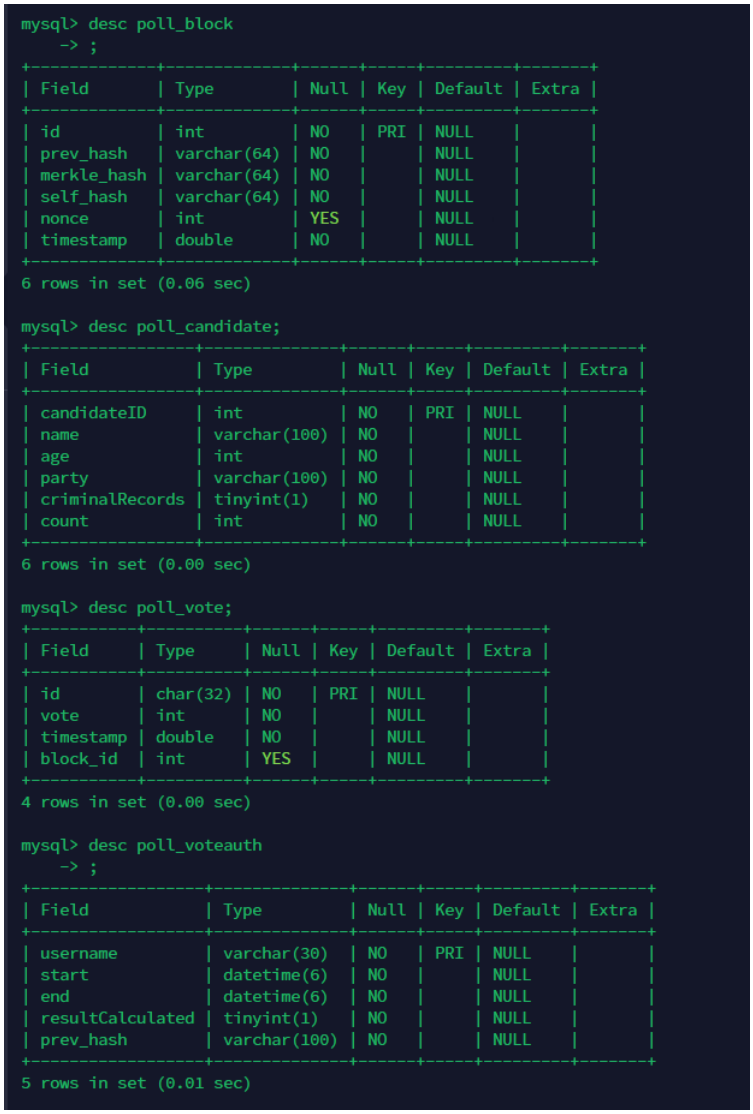
Api ninja is used for generating secret passphrases .this enhances the security as we are generating random passphrases from 3rd party.

## 5.5 Database Design

```
mysql> show tables;
+----------------------------+
| Tables_in_zvote_db         |
+----------------------------+
| auth_group                 |
| auth_group_permissions     |
| auth_permission            |
| auth_user                  |
| auth_user_groups           |
| auth_user_user_permissions |
| django_admin_log           |
| django_content_type        |
| django_migrations          |
| django_session             |
| poll_block                 |
| poll_candidate             |
| poll_vote                  |
| poll_voteauth              |
| poll_voter                 |
| poll_voterlist             |
| poll_voterpvt              |
+----------------------------+
17 rows in set (0.00 sec)

mysql>
```

Figure 5.17: All Tables

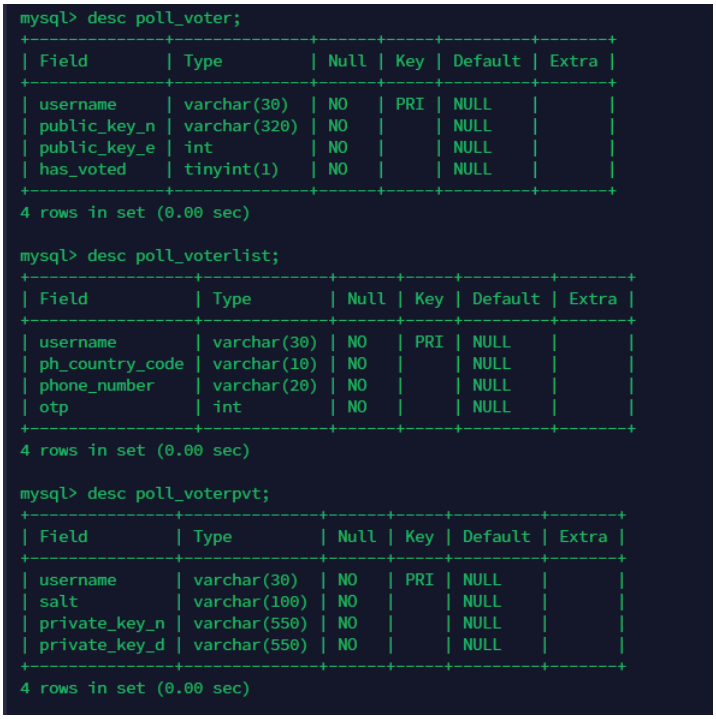
In this context, the voter's username serves as the primary key.



```
mysql> desc poll_block
    -> ;
+-------------+-------------+------+-----+---------+-------+
| Field       | Type        | Null | Key | Default | Extra |
+-------------+-------------+------+-----+---------+-------+
| id          | int         | NO   | PRI | NULL    |       |
| prev_hash   | varchar(64) | NO   |     | NULL    |       |
| merkle_hash | varchar(64) | NO   |     | NULL    |       |
| self_hash   | varchar(64) | NO   |     | NULL    |       |
| nonce       | int         | YES  |     | NULL    |       |
| timestamp   | double      | NO   |     | NULL    |       |
+-------------+-------------+------+-----+---------+-------+
6 rows in set (0.06 sec)

mysql> desc poll_candidate;
+-----------------+--------------+------+-----+---------+-------+
| Field           | Type         | Null | Key | Default | Extra |
+-----------------+--------------+------+-----+---------+-------+
| candidateID     | int          | NO   | PRI | NULL    |       |
| name            | varchar(100) | NO   |     | NULL    |       |
| age             | int          | NO   |     | NULL    |       |
| party           | varchar(100) | NO   |     | NULL    |       |
| criminalRecords | tinyint(1)   | NO   |     | NULL    |       |
| count           | int          | NO   |     | NULL    |       |
+-----------------+--------------+------+-----+---------+-------+
6 rows in set (0.00 sec)

mysql> desc poll_vote;
+-----------+----------+------+-----+---------+-------+
| Field     | Type     | Null | Key | Default | Extra |
+-----------+----------+------+-----+---------+-------+
| id        | char(32) | NO   | PRI | NULL    |       |
| vote      | int      | NO   |     | NULL    |       |
| timestamp | double   | NO   |     | NULL    |       |
| block_id  | int      | YES  |     | NULL    |       |
+-----------+----------+------+-----+---------+-------+
4 rows in set (0.00 sec)

mysql> desc poll_voteauth
    -> ;
+------------------+--------------+------+-----+---------+-------+
| Field            | Type         | Null | Key | Default | Extra |
+------------------+--------------+------+-----+---------+-------+
| username         | varchar(30)  | NO   | PRI | NULL    |       |
| start            | datetime(6)  | NO   |     | NULL    |       |
| end              | datetime(6)  | NO   |     | NULL    |       |
| resultCalculated | tinyint(1)   | NO   |     | NULL    |       |
| prev_hash        | varchar(100) | NO   |     | NULL    |       |
+------------------+--------------+------+-----+---------+-------+
5 rows in set (0.01 sec)
```

Figure 5.18: Block,Candidate,Vote,Vote authentication Table Structure

Block table stores blokchain based data like merkle hash,previous hash,self hash and time.Candidate table stores candidate id,age,party,criminal record.Vote table is used to store data of vote like timestamp,block which the vote is stored.Voteauth table stores starting time and ending time of vote,data on whether the data is calculated or not.



```
mysql> desc poll_voter;
+--------------+--------------+------+-----+---------+-------+
| Field        | Type         | Null | Key | Default | Extra |
+--------------+--------------+------+-----+---------+-------+
| username     | varchar(30)  | NO   | PRI | NULL    |       |
| public_key_n | varchar(320) | NO   |     | NULL    |       |
| public_key_e | int          | NO   |     | NULL    |       |
| has_voted    | tinyint(1)   | NO   |     | NULL    |       |
+--------------+--------------+------+-----+---------+-------+
4 rows in set (0.00 sec)

mysql> desc poll_voterlist;
+-----------------+-------------+------+-----+---------+-------+
| Field           | Type        | Null | Key | Default | Extra |
+-----------------+-------------+------+-----+---------+-------+
| username        | varchar(30) | NO   | PRI | NULL    |       |
| ph_country_code | varchar(10) | NO   |     | NULL    |       |
| phone_number    | varchar(20) | NO   |     | NULL    |       |
| otp             | int         | NO   |     | NULL    |       |
+-----------------+-------------+------+-----+---------+-------+
4 rows in set (0.00 sec)

mysql> desc poll_voterpvt;
+---------------+--------------+------+-----+---------+-------+
| Field         | Type         | Null | Key | Default | Extra |
+---------------+--------------+------+-----+---------+-------+
| username      | varchar(30)  | NO   | PRI | NULL    |       |
| salt          | varchar(100) | NO   |     | NULL    |       |
| private_key_n | varchar(550) | NO   |     | NULL    |       |
| private_key_d | varchar(550) | NO   |     | NULL    |       |
+---------------+--------------+------+-----+---------+-------+
4 rows in set (0.00 sec)
```

Figure 5.19: Voter,Voterlist,Voter privatekey Table Structure

Voter table stores the public keys of the voter and to store the condition whether the voter is voted or not.Voterlist table stores the username,phone number,country code. Voterpvt table stores username and hashed private keys of the voter.

## 5.6 Technology Stack

- **Front-end Development**

  HTML/CSS: For creating the website's structure and styling.

  Bootstrap: For creating visually appealing and consistent user interfaces.It provides a collection of CSS, JavaScript, and pre-designed HTML components

- **Back-end Development**

  Django Web Framework : Django is a popular open-source web framework written in Python. It provides a robust set of tools and features for developing web applications quickly and efficiently.

  MySQL : MySQL is an open-source relational database management system (RDBMS) that is widely used for storing and managing structured data. It is one of the most popular database systems in the world, known for its performance, scalability, and ease of use.

  Nginx: It is a high-performance, open-source web server software known for its efficiency, speed, and scalability. It is commonly used as a reverse proxy server, load balancer, and HTTP cache, but it can also function as a web server for serving static content or as a proxy for various protocols.

  Gunicorn : It is a Python Web Server Gateway Interface (WSGI) HTTP server. The purpose of Gunicorn is to act as a bridge between the web server and the Python web application.

  Merkle tree: A Merkle tree, also known as a hash tree, is a data structure used in computer science and cryptography to efficiently verify the integrity and consistency of a large amount of data.

- **Other Tools and Technologies**

  Git: A version control system for tracking changes in code and collaborating with other developers.

  GitHub : Online platforms for hosting and managing.

  Redis (Remote Dictionary Server): Redis is an open-source, in-memory data structure store and caching system.

  API:API stands for Application Programming Interface. It is a set of rules and protocols that allows different software applications to communicate and interact with each other.

  Cryptography module: It is a Python library that provides cryptographic functionality to developers for secure data encryption, decryption, hashing, and other cryptographic operations.

# CHAPTER 6

# IMPLEMENTATION

## 6.1 Proposed Work

During the implementation phase of Z VOTE, the proposed work involved several key steps and activities:

- User Authentication: Implement user registration and login functionalities to manage the electoral process.
- Blockchain implementation: e-voting system can use blockchain to maintain a decentralized and tamper-resistant voter registration database. Each eligible voter can have a unique cryptographic identity recorded on the blockchain.
- Encryption Implementation: Encryption in a blockchain is typically applied to secure sensitive data, such as transaction details or private keys, from unauthorized access.
- API Implementation: APIs (Application Programming Interfaces) are crucial for enabling seamless integration, data retrieval, and interaction between the blockchain and external systems.

## 6.2 Module Description

Our project Z VOTE contains 3 modules, they include the website user page, database and API.

**User pages :** The website contains 2 user pages, one for the voter and the other for the voting authority. Through the voter user page, the voter can register themselves.After registration and login verification the voter can cast vote.

The voting authority user page allows the voting authority to monitor the voting process,voting authority can add voters and candidates and they can set the voting time.

**Database :** Using MySQL for sorting voters information,candidate information,voting time information,Block information and vote information.

**API's :** API's are used for passphrase generation and sms authentication.

**Voting Authority:**

- Voting Time:Voting authority set the voting time.The voter can Register,Login,and vote only within the time limit fixed by the voting authority.
- Result Calculation:The final result is calculated by the voting authority based on the votes cast by the participants.
- Voter List:The voting authority assumes responsibility for managing the voting list, meticulously verifying the eligibility of individuals for voting. If an individual is deemed eligible, they are promptly added to the voter list, granting them the right to cast their vote.
- Vote monitoring:Voting authority has an exclusive authority to monitor the vote.
- Candidate list:Voting authority manages the candidate list.They checks whether a candidate is eligible to conduct in an election and add them to the candidate list.
- Verification and Result:The voting authority holds the exclusive authority to verify votes and determine the final result.

**Voter:**

- Voter Registration:When the voter register an OTP is send to the registered phone number of the voter.Using this OTP voter can set a new password.Then a secret passphrase is authomatically generated by third party api.
- Voter Login:Upon registration, voters can log in to the system using the username and password they have set. Subsequently, upon successful login, the system will redirect the voter to the voting page, allowing them to participate in the voting process.
- Voting: After a voter successfully authenticates themselves using a secret passphrase, they gain the ability to cast their vote. Following the voting process, the voter has the option to seal the ballot, and subsequently, they are provided with a unique ID as a reference for their vote.
- Vote verification: After the voting process is completed, voters are given the opportunity to verify their vote by utilizing the unique ID generated for their ballot.
- Result:Voters have the option to check the result of the election, which will be made visible exclusively after the designated voting time, predetermined by the voting authority, has elapsed.

## 6.3 Data-Set

**Voter List:** This dataset comprises a comprehensive list of voters, including the voter's username, phone country code, and their registered phone number.

**Candidate list:** This dataset consists of an extensive collection of candidates, encompassing candidate ID, candidate age, and the affiliated political party of each candidate.

# CHAPTER 7

# RESULTS

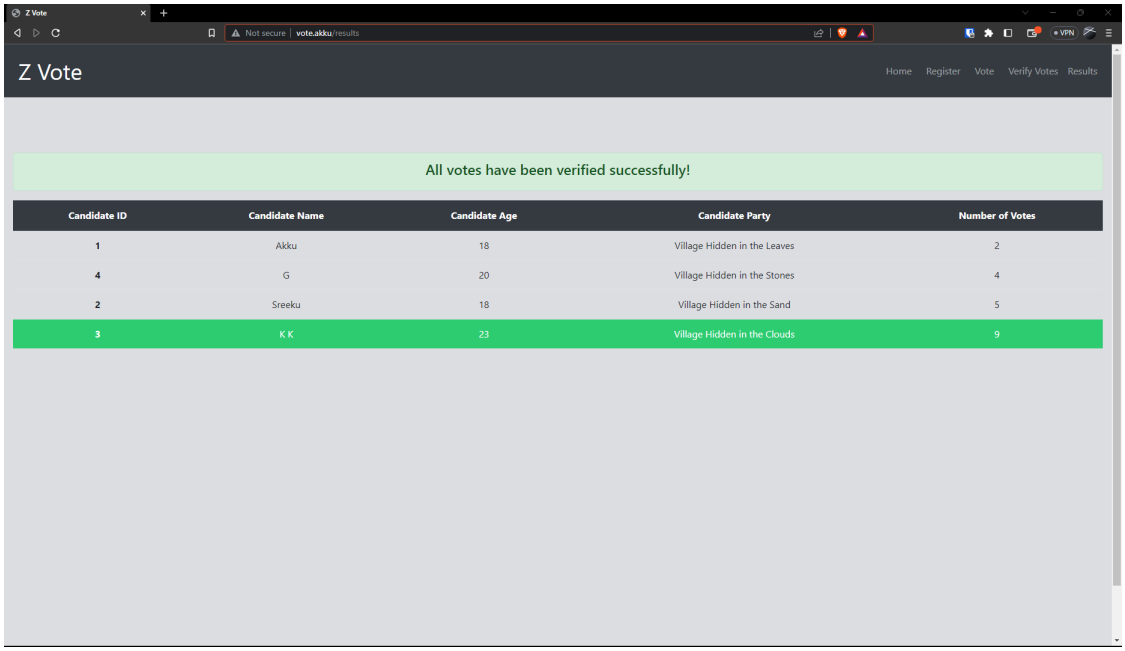



Figure 7.1: Result Page

The winning candidate will be highlighted in a distinctive green color, making it easily identifiable.

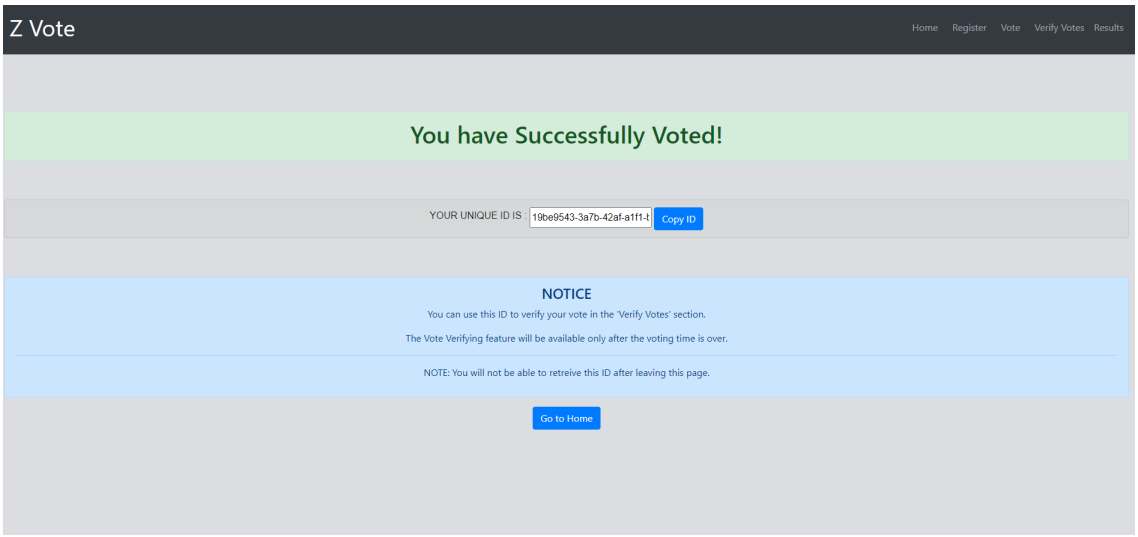



Figure 7.2: Vote Successful

Vote Successful page(refer to Fig 7.2) make sure voting is successful or not.This page gives you the unique id which voter can use to verify their vote.

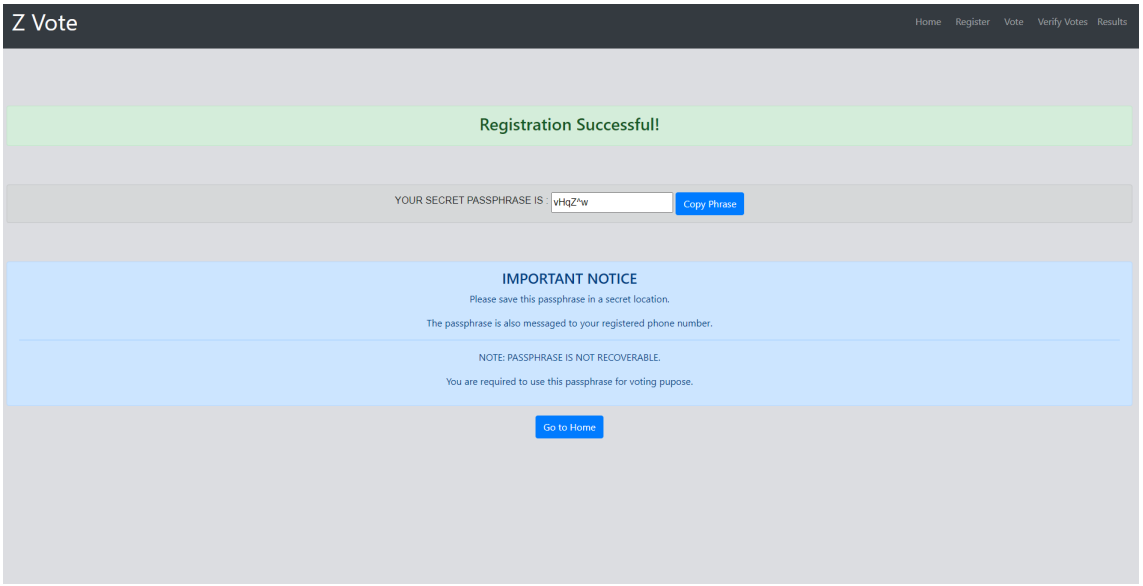



Figure 7.3: Registration Successful

At this stage, an essential element known as the secret passphrase is generated (refer to Fig 7.3). This passphrase serves as a crucial key for the voting process, ensuring security and authenticity

# CHAPTER 8

# CONCLUSION AND FUTURE SCOPE

## 8.1 Conclusion

Blockchain based e-voting system ensures transparency, security, and immutability of votes. Each vote is recorded on the blockchain, creating a tamper-proof and auditable record of the entire voting process. This increases trust and confidence in the system by minimizing the potential for fraud and manipulation. The decentralized nature of blockchain eliminates the need for a central authority, reducing the risk of bias and corruption. It allows for a distributed network of nodes to verify and validate votes, making it difficult for any single entity to control or manipulate the outcome. Additionally, the use of cryptographic algorithms in blockchain-based e-voting systems ensures the privacy and anonymity of voters. It allows individuals to cast their votes without revealing their identity, protecting their rights and maintaining confidentiality. In conclusion, a blockchain-based e-voting system offers enhanced security, transparency, privacy, and accessibility compared to traditional voting systems. While there are still technical and logistical challenges to overcome, the potential benefits make it a promising solution for improving the integrity and efficiency of democratic elections.

## 8.2 Future Scope

Looking ahead,the future of blockchain based e-voting system holds immense potential. Governments and electoral authorities may start considering blockchain technology as a viable solution to enhance the integrity and transparency of the voting process. Future advancements may involve integrating blockchain-based e-voting systems with robust identity management systems. The global nature of blockchain technology opens up opportunities for international collaboration in the development of e-voting systems. Mobile apps could be developed to provide a user-friendly interface for voting, while biometric authentication methods, such as fingerprint or facial recognition, could be employed for secure voter identification.

# REFERENCES


[1] **Nir Kshteri**, , and **Jeffery Voas**, "Blockchain-Enabled E-Voting," in *IEEE Software ( Volume: 35, Issue: 4, July/August 2018).*

[2] **CHjalmarsson**, **Friorik P.**, **Gunnlaugur K. Hreioarsson**,**Mohammad Hamdaqa**,and **Gisli Hjalmtysson.** "Blockchain-Based E-Voting System.," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986. IEEE, 2018.*

[3] **Hsin-Te Wu**,and **Chang-Yi Yang** "LA Blockchain-Based Network Security Mechanism for Voting Systems.," in *2018 1st International Cognitive Cities Conference (IC3).*

[4] **Basit Shahzad, and Jon Crowcroft,** "Trustworthy Electronic Voting Using Adjusted Blockchain Technology," in *IEEE Access ( Volume: 7) on 24 February 2019 .*

[5] **Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam and Sajib Ahamed** "DVT Chain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system," in *01 October 2022 Publication History.*

[6] **Uzma Jafar,Mohd Juzaiddin Ab Aziz,Zarina Shukur and Hafiz Adnan Hussain** "Scalable Blockchain-Based Electronic Voting Systems," *Published online 2021 Aug 31. doi: 10.3390/s21175874.*

[7] **"PyCryptodome python based library which contains basic encryption functions "** [Online] : https://pycryptodome.readthedocs.io/en/latest/src/introdu ction.html .

[8] **"Django documentation"** [Online] : https://docs.djangoproject.com/en/3.0/.

[9] **"Blockchain Technology"** [Online] : https://www.investopedia.com/terms/b/blockchain.asp.

[10] **"Python learning"** [Online] : https://docs.python.org/3/tutorial/index.html.