DE-41 (EE)

Muhammad Talha, Muneeb Mubashir, Fawad Khan Afridi, Mahnoor Shakir

Secure E-Voting Machine Employing Blockchain Network & Computer Vision

COLLEGE OF
ELECTRICAL AND MECHANICAL ENGINEERING
NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY
RAWALPINDI
2023

CERTIFICATE OF APPROVAL

It is to certify that the project "**Secure E-Voting Machine Employing Blockchain Network & Computer Vision**" was done by **NS Muhammad Talha, NS Muneeb Mubashir, NS Fawad Khan Afridi, NS Mahnoor Shakir** under the supervision of **Sobia Hayee.**

This project is submitted to the **Department of Electrical Engineering**, College Of Electrical and Mechanical Engineering (Peshawar Road Rawalpindi), National University of Sciences and Technology, Pakistan in partial fulfillment of Requirements for the degree of Bachelor of Engineering in Electrical Engineering.

Students:

1-Muhammad Talha

NUST ID: _____ Signature: _____

2-Muneeb Mubashir

NUST ID: _____ Signature: _____

3-Fawad Khan Afridi

NUST ID: _____ Signature: _____

4-Mahnoor Shakir

NUST ID: _____ Signature: _____

APPROVED BY:

Project Supervisor: _____ Date: _____

Sobia Hayee

DECLARATION

We affirm that the content presented in this Project Thesis is original and has not been submitted in support of any other degree and qualification at this and any other educational institution. We acknowledge that any act of plagiarism will result in full responsibility and may lead to disciplinary action, including the potential cancellation of our degree, based on the severity of the offense.

1. M. Talha _____
2. Muneeb Mubashir _____
3. Fawad Khan Afridi _____
4. Mahnoor Shakir _____

ACKNOWLEDGMENTS

We would like to acknowledge everyone who played a role in our academic achievements.

First thanks to Allah Almighty, and our parents who loved and supported us in throughout our lives, especially through our academic endeavors, without their constant support we would not have been so fortunate.

Secondly, the faculty and especially our supervisors who guided us on every wrong turn and helped us see the error in our ways.

The vast experience of our teachers and their constant advice helped us prevent errors which could not have foreseen throughout the research process and the implementation phase.

Thank you all for your unwavering support.

ABSTRACT

Voting in a democratic election is a solemn and significant occasion worldwide. Paper ballots or electronic voting machines are used in today's elections, whether in a school, college, or even a country. This system has various disadvantages, including a lack of transparency, low voter turnout, vote manipulation, distrust of election authorities, delays in results, and, most crucially, security issues.. Therefore, the development of digital technology today has improved the lives of many. To counteract the drawbacks of the current voting method, electronic voting is proposed. In essence, electronic voting is a way to cast and tally ballots electronically. It is a quick, inexpensive, and secure approach to carry out a voting process that demands high security and is data-rich and real-time. Concerns concerning the privacy of communications and network security for electronic voting have grown recently. As a result, the availability of electronic voting is urgently needed and is growing in popularity in networking and communication. Blockchain technology is one solution to address security issues. . In order to establish a blockchain and computer vision based electronic voting system, this article proposes a new method that resolves some of the shortcomings of existing systems and evaluates some of the most prominent blockchain frameworks. Since the blockchain maintains its data in a decentralized manner, the outcome of the implementation demonstrates that the blockchain is a viable and secure electronic voting system that resolves the problem of vote falsification in electronic voting. Blockchain-based electronic voting can be utilized by direct network applications.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

SUSTAINABLE DEVELOPMENT GOALS

Pakistan reaffirmed its commitment to the 2030 plan for Sustainable Development by adopting the Sustainable Development Goals (SDGs) as its own national development plan through a unanimous National Assembly Resolution in 2016. Since then, the government has made considerable advancements by integrating these goals into national policies and programs and developing an institutional framework for Pakistan's implementation of the SDGs.

OUR FYP SDG's:

- **Industry, Innovation & Infrastructure:**

This is one of the 17 Sustainable Development Goals (SDGs) listed in the United Nations' 2030 Agenda for Sustainable Development in 2015. The goals are to build strong and sustainable infrastructure, advance inclusive and sustainable industrialization, and encourage innovation.

Governments, the business sector, and civil society organisations must collaborate in order to invest in infrastructure that promotes sustainable development, job creation, and economic progress. This may entail increasing renewable energy sources, enhancing transit networks, and making investments in telecommunications infrastructure to close the digital gap.

Innovation is essential to accomplishing this objective since it advances the creation of new technology, procedures, and goods that increase productivity and cut waste. The objective supports the emergence of sustainable and inclusive business models that advance social and economic development while protecting

the environment.

By encouraging economic growth and job creation while ensuring that the benefits are distributed evenly and sustainably across all sectors of society, the accomplishment of this aim will ultimately contribute to the overarching goal of sustainable development.

- **Peace, Justice & Strong institution:**

The goal aims to promote peaceful and inclusive societies, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels.

To achieve this goal, governments, civil society organizations, and other stakeholders must work together to promote good governance, transparency, and accountability. This includes strengthening the rule of law, promoting access to justice for all, combating corruption and bribery, and building effective, inclusive, and accountable institutions at all levels of government.

The goal also seeks to promote peaceful and inclusive societies by addressing the root causes of conflict and violence, promoting social cohesion, and ensuring that all people have equal access to political, economic, and social opportunities. This includes promoting the participation of women and marginalized groups in decision-making processes and ensuring that their rights are protected.

- **Reduced Inequalities:**

Reduced Inequalities, or SDG 10, is a Sustainable Development Goal with the dual objectives of reducing inequality of all kinds and fostering social inclusion. It ixecentrali reducing income disparity, advancing equality of opportunity, and empowering disadvantaged populations. Progressive taxation, social safety nets, inclusive ixecentralize, equitable access to services, and anti-discrimination laws and regulations are only a few examples of initiatives. The objective is to build a more just society where everyone has access to resources and fair opportunities.

4.2 Aim of the project

A web-based voting system called an online voting system can make managing elections easier and more secure. Voting may be done using this approach during elections conducted at universities and other places. It employs facial recognition technology to authenticate the user, solving the issue of fake entries. As a result, this technique ensures that there can be no election fraud and that voting will be simple, requiring voters to stay inside to cast their ballots.

1.2 Project Scope

Transparent transaction using Blockchain technology increases the security of the transaction of crypto that races towards cybersecurity.

The information is all safe and accurate. Cryptography is used to encrypt data in order to remove risks like 10ecentralize data tampering, which would boost cryptocurrency payments.

1.3 Project Objectives

•The basic goals of E-voting systems are to speed up the counting of votes, reduce the cost of hiring people to count votes by hand, and make voting more accessible for people with disabilities.

• This may be achieved by conceiving of and developing a software platform that facilitates the registration of voters, the casting of votes in elections, the collection and real-time monitoring of election results, and, most importantly, the participation of voters from afar.

• Blockchain technology will be 10ecentra to study and build a security approach that will be used to assure that votes placed in the system won’t be hacked and won’t be subject to outside assault.

1.4 Project Modules

1. Login Module
2. Voting Module

3. Voting Creation Module
4. Voting Result Module
5. User Identification Module

1.5 Project Basic Requirements

1.5.1 Hardware Requirements

- Any device containing camera with high processing power.

1.5.2 Software Requirements

- Front-End: React-js
- Back-End: Node-js, Express-js, Solidity
- Blockchain: MetaMask, Ganache
- Others: Domain name, Hosting, sever and cloud storage

1.5.3 Software requirements for our clients

- Windows 7 or higher OS
- Google chrome or any other safe browser
- Good Internet Speed
- Blockchain ID with sufficient Ethereum

Chapter 2: Literature review

2.1 Introduction

Blockchain is a decentralized technology that enables the secure and transparent storage and transfer of data. It serves as the underlying technology for cryptocurrencies like Bitcoin and has far-reaching applications beyond just digital currencies.

- Distributed Ledger: Blockchain operates as a distributed ledger, where multiple participants, known as nodes, maintain and update a shared database. Each node has a copy of the entire blockchain, ensuring redundancy and eliminating the need for a central authority.
- Blocks: Information on the blockchain is grouped into blocks, which contain a set of transactions or data. Each block typically includes a unique identifier (hash), a timestamp, and a reference to the previous block, creating a chronological chain.
- Cryptographic Hashing: Blocks in the blockchain are linked together using cryptographic hashes. A hash is a unique string of characters generated by a mathematical algorithm. Any change in the data of a block will result in a different hash, making it tamper-evident.
- Consensus Mechanism: Consensus mechanisms enable nodes in the network to agree on the state of the blockchain and validate new transactions. Popular consensus algorithms include Proof of Work (PoW) and Proof of Stake (PoS), which ensure that participants reach agreement without a central authority.
- Immutable and Transparent: Once a block is added to the blockchain, it becomes nearly impossible to alter or delete the data contained within it. This immutability enhances the security and integrity of the stored information. Moreover, the blockchain's transparency allows anyone to view and verify the transactions, promoting trust and accountability.
- Smart Contracts: Blockchain platforms like Ethereum introduced the concept of smart contracts, which are self-executing agreements with predefined conditions. Smart contracts automate transactions and eliminate the need for intermediaries, offering enhanced efficiency and reducing costs.

The applications of blockchain extend beyond cryptocurrencies, including:

1. Financial Services: Blockchain can streamline cross-border payments, enhance identity verification, facilitate smart contracts for insurance and derivatives, and improve auditing and compliance processes.

2. Supply Chain Management: Blockchain can provide end-to-end visibility and traceability, reducing fraud and counterfeiting, optimizing inventory management, and ensuring ethical sourcing.
3. Healthcare: Blockchain can securely store and share medical records, enable interoperability between healthcare providers, facilitate drug traceability, and improve clinical trials' transparency.
4. Voting Systems: Blockchain can enhance the integrity and transparency of voting processes, making them more resistant to tampering and fraud.
5. Energy and Utilities: Blockchain can enable peer-to-peer energy trading, track renewable energy generation and consumption, and streamline billing and grid management.
6. Intellectual Property: Blockchain can establish provenance for digital assets, protect copyrights, and enable decentralized content distribution platforms.

These are just a few examples of how blockchain technology is revolutionizing various industries by providing trust, security, and efficiency in the digital age.

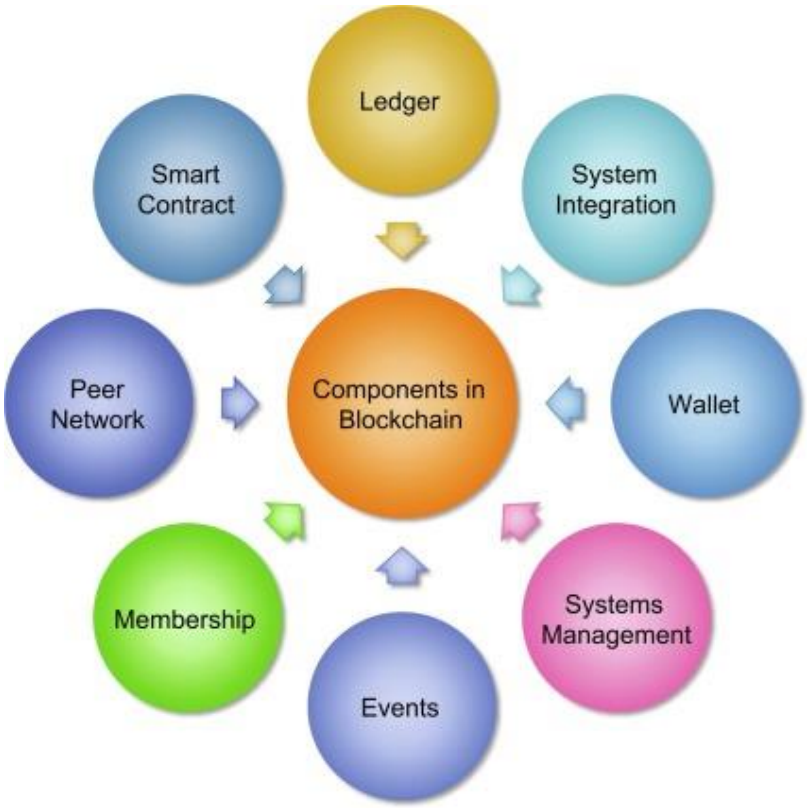


Figure 1 Blockchain Core Component

Chapter 3: Analysis, Design Methodology and Implementation Strategy

3.1 Project Feasibility study

The feasibility study evaluates how useful or practicable the system's development will be to the organization. It serves as the Systems Investigation's preliminary survey. It tries to offer details that will make a subsequent in-depth inquiry easier. The report created at the conclusion of the feasibility study includes recommendations and well-reasoned defenses to aid management in determining whether to allocate more funds to the proposed project.

3.1.1 Economical Feasibility

In the economic feasibility study, the cost of creating the system is compared to the end benefit gained from the new systems. The financial value of the benefits must at least equal the cost of the investments. If the system can be designed with an accuracy of 95% or above, it will be cost-effective to implement.

3.1.2 Technical Feasibility

This is the investigation of how a system works, how well it performs, and the limits placed upon it. To conduct this feasibility research, we looked at whether or not it would be viable to use a variety of frontend and backend platforms to provide the full set of features outlined in the System Requirement Specification (SRS).

3.1.3 Operational Feasibility

The suggested system is, without a doubt, entirely graphical user interface oriented, making it incredibly user pleasant and making all inputs to be taken self-explanatory even to a layperson. In addition, users have been provided with in-depth training to 14ecentraliz them with the new interface. Our research indicates that customers are satisfied with the solution since it has reduced their workload.

3.2 Detailed Module Description

3.2.1 Login

This module describes about login functionality in which there are two types of logins are there 1) User Login 2) Admin Login**.**

3.2.2 Voting

In this module users can cast their votes. This module will describe a whole page where there will be a list of candidates were noted with their symbols.

3.2.3 Voting Creation

In admin can create whole voting environment (i.e., arrange voting facility, specifies time of voting, add candidates that have stand, and records the entry that particular person has voted, etc.).

3.2.4 Voting Result

This module is the main module of our system as it gives the result of the voting. As we have used blockchain technology our votes will not be altered and thus purity maintains and the proper candidate will be won.

3.2.5 User Identification

This module system will authenticate to the user that particular user is valid or not. This authentication will be done by face recognition system where user will have to scan their face to access the voting portal to make voting system crystal clear because due to this no other person can cast vote in place of a particular user.

3.3 Project SRS

3.3.1 Class Diagram

Classes are used to describe collections of items that have similar properties, behaviours, associations, and meanings.

- **Symbols**

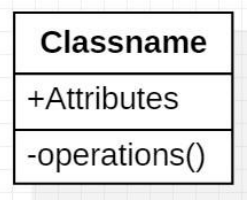
	Classname: The only mandatory tag in a class's visual representation is "classname," which is the name of the class. The top drawer is where you can always find it. Attribute: A class attribute is a piece of information about the modelled object that is referred to by name. Attributes are shown in the class diagram's second box, which is located just beneath the name box. Attributes can be: + public. # Protected - private / Derived Operation: Operations describe the class behaviour and appear in the third compartment.

Table 1 Class Diagram Symbol Table

- **Diagram**

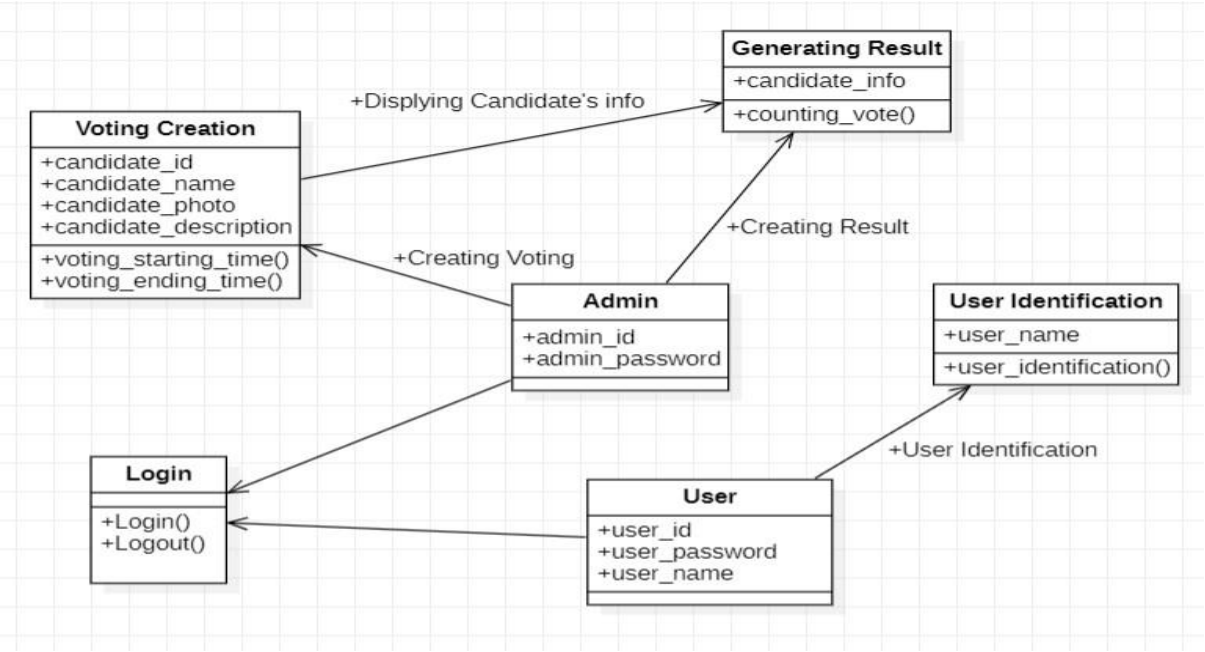


Figure 2 Class Diagram

3.3.2 Use-case Diagram

A software system's primary features may often be explained with the help of a use case diagram. Use case diagrams are a graphical depiction of user interactions with a system, outlining the connection between the user and the many use cases that involve the user. A use case diagram, which is commonly supplemented by other diagram types, may identify the various users of a system and the many use cases.

Use cases are simply documented examples of how a system is supposed to work. Now, actors are another topic that is important to the use cases. An actor is anything that participates in the system in some way.

In a nutshell, use case diagrams provide the following functions:

1. Used for determining what features a system must have.
2. Employed to gain a holistic perspective on a setup.
3. Recognize the system's internal and external influences.
4. Illustrate how the criteria function as players in the play.

• **Symbols**

	In a use case diagram, a user is represented by a simple stick figure. One or more use cases involve each player.
 Use Case	Interacting parties beyond the information system itself, such as humans, processes, or other computerized systems.

Table 2 Use Case Diagram Symbol Table

• **Diagram**

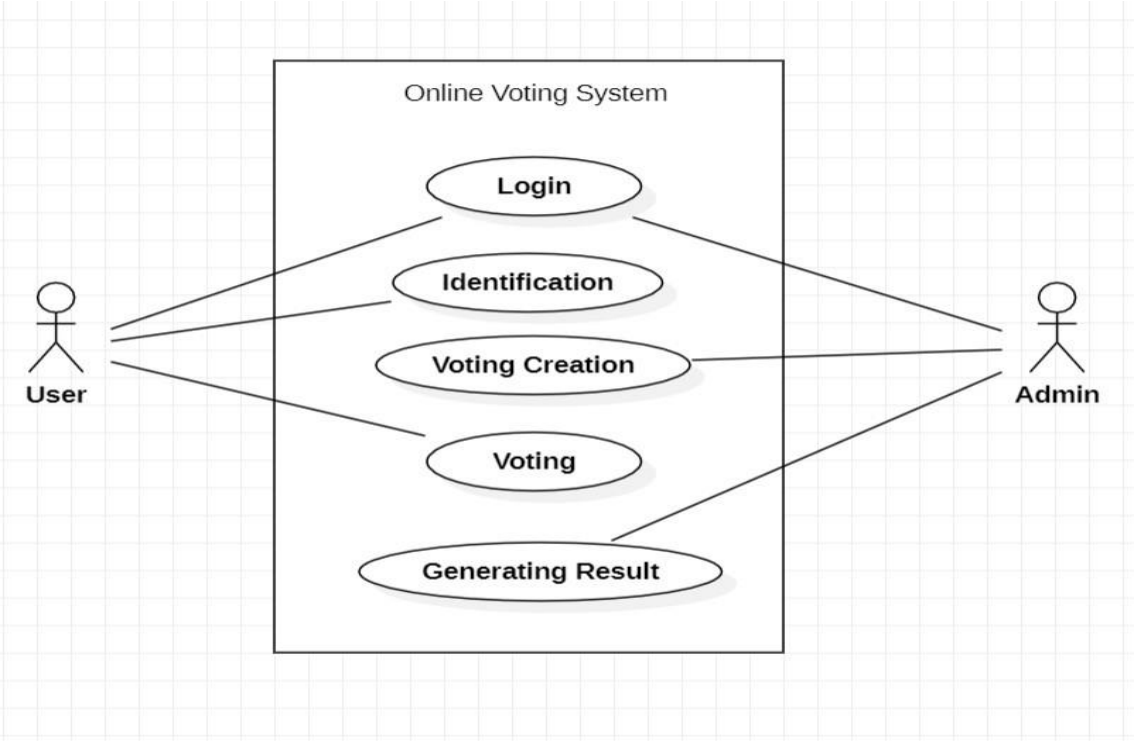


Figure 3 Use Case Diagram

3.3.3 Event Trace Diagram

Event Trace diagrams are straightforward representations of sequentially occurring

interactions between objects. Meaning the chronological arrangement of these exchanges. A sequence diagram can also be referred to as an event diagram or a scenario of possible events.

• **Symbols**

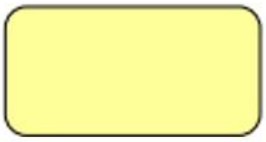
	Start State
	Final State
	Simple State

Table 3 Event Trace Diagram Symbol Table

Flowchart:

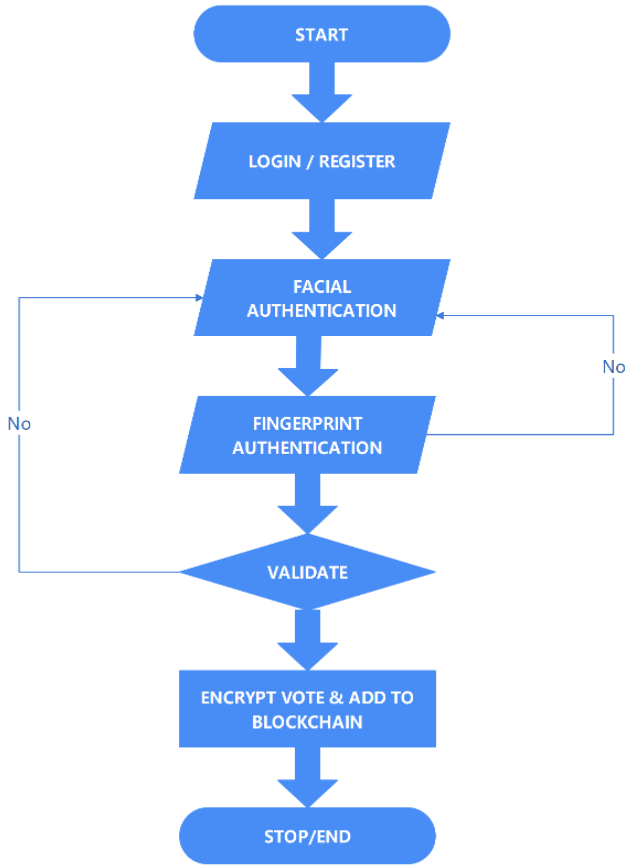


Figure 4 Event Trace Diagram

3.3.4 State Diagram

Graphical representations of the behavior of systems using state diagrams are commonplace in computer science and related fields. There are two cases: either the system actually has a finite number of states, or the number of states is an appropriate abstraction. There are several varieties of state diagrams, each with its own unique syntax and meaning.

Block Diagram

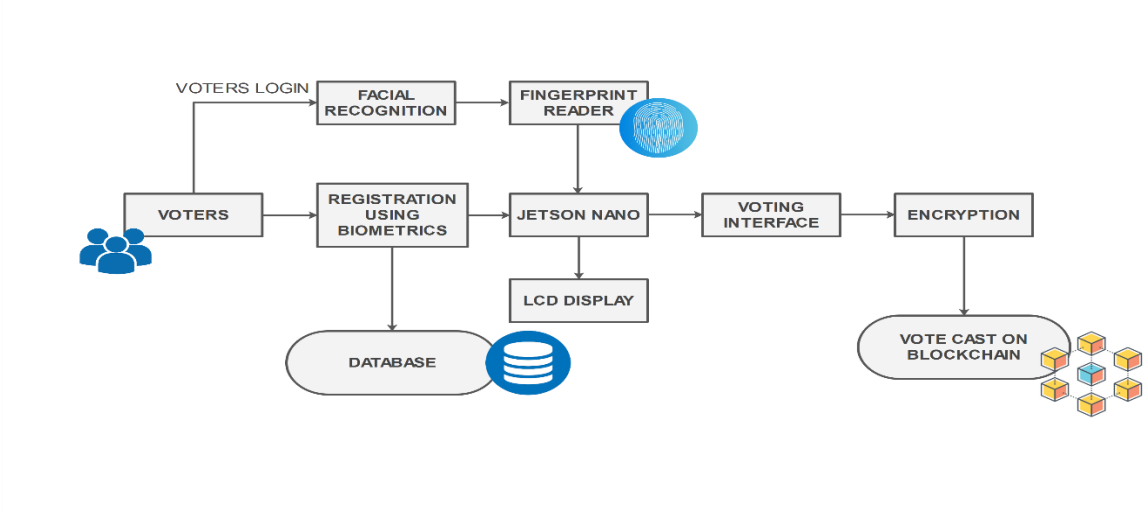


Figure 5 State Diagram

3.4 Methodology

In this part, we will demonstrate the preliminary stages of our application's design and functionality. The user visits the website where the platform is housed and registers and votes in a safe and open environment. The procedure is described in detail below.

3.4.1 Registration Stage

At this point, the voter must provide his or her Aadhar number, email address, name, and phone number in order to register to vote. Because authentication in this system is based on face recognition, they must also provide a high-quality photo of themselves.

3.4.2 Login

The voter then attempts to log in and cast his vote after registering. The first step in the voting process requires the voter to provide a password. After logging in, the voter must authenticate before casting a ballot. Facial recognition technology is utilized for instantaneous authentication to boost safety.

3.4.3 Blockchain Technology

Security is the primary use for this technology. Blockchain creates an atmosphere that is safe and open to all parties involved. Blockchain uses an asymmetric encryption technique to encrypt the voter's message (Casted vote). The Blockchain supplies the public key, and the host has the private. To verify your identity when accessing the ledger, use the public key.

3.4.4 Ethereum

The Ethereum network serves as a platform upon which the blockchain may be built and stored. The information about each block is generated and kept in a secure ledger. High fault tolerance is achieved by distributing these created blocks throughout the nodes. A voter who doesn't utilize Ethereum can't cast a vote. This is why ganache is utilized. Ganache is an implementation of the Ethereum blockchain that may be used to communicate with smart contracts on a private blockchain in a manner similar to Ethereum.

3.4.5 Database

The MongoDB database stores all system data. Voter names and ID numbers, as well as other voting-related information like polling location, day, and hour, will all be collected.

3.4.6 Admin

The entire system will be under Admin's command. The administration will check the eligibility of voters and candidates. Voting schedules are set by admin alone. Administrative control extends to critical communications like results and the like.

3.4.7 Results Phase

In the results phase, ballots are processed and counted. The outcomes are created and shown on the online platform. Votes cast by users can be validated by using their public keys. This guarantees that the voting process is open and honest.

3.4.8 Meta Mask

Users of the blockchain may control their funds via MetaMask. Users may access the wallet and make transactions directly from their browser by installing the associated add-on. A meta mask appears whenever a transaction is made, prompting the user to approve the activity.

3.4.9 Truffle

MetaMask allows users on the blockchain to manage their own cash. When the related browser extension is installed, users may access the wallet and conduct transactions without ever leaving their browser. Every time a purchase is completed, a meta mask pops up to ensure the user is okay with the action.

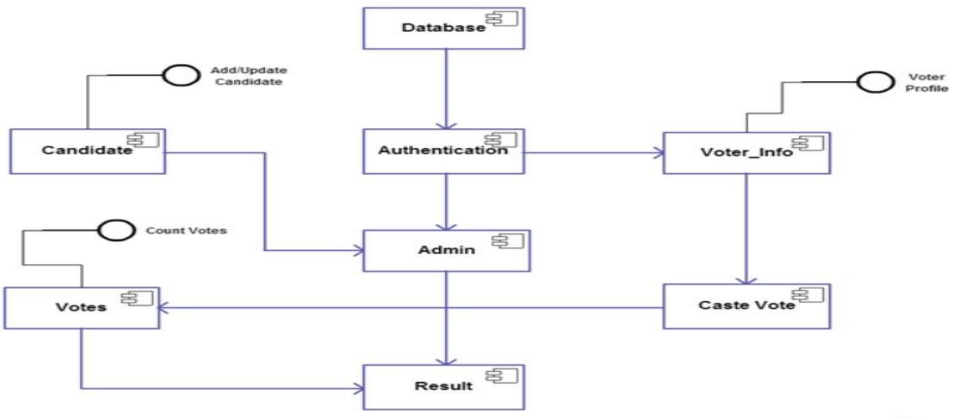


Figure 6 Overview of System

3.5 Voting Process

Based on the present state of the system, we now detail a user's usual experience interacting with the proposed method. The voter essentially signs into the system by having their face scanned. The voter's identity is confirmed by the system after a facial scan. If a voter's preferences are discovered to be similar to those of a candidate, the voter will be shown a selection of opposing candidates. If the match is not successful, on the other hand, access will be revoked. Authentication (in this example, a facial recognition system) and role-based access control that have been properly implemented allow for this feature to be realized. Additionally, it is assumed that each voter is allotted a certain electoral district, and that this information is utilized to generate a list of candidates from which the voter may make their selection. Due to the offline nature of voter registration, it is not possible to include that process in this research.

Votes are uploaded to the public ledger once they have been cast successfully and mined by several miners for verification. Blockchain technology employs cryptographic hashes to secure end-to-end verification, making voting a particularly safe process. On this context, a vote counts as a transaction on the blockchain of the voting app. As a result, the deciding vote is recorded in the final tables of the database and included as a new block in the blockchain (after successful mining). The system guarantees that no two people may possess voting machines or control the same vote. A matching voter face is used at the beginning of each voting attempt to ensure that only once has been counted. When miners "mine" a vote, a separate transaction is created for each vote. A malicious vote will result in the miner being disqualified.

As soon as the validation procedure is complete, the user will get a notice by message or email including the transaction ID described above. While this fulfills its job as a voter alert, it prevents anybody from learning how an individual voter cast their ballot. An individual voter is identified on the blockchain by their cryptographic hash, which is their unique hash. The entire voting process can be more easily verified thanks to this addition. In addition, this id is encrypted so that not even the system operator or administrator can see it, protecting voters' privacy.

3.6 Blockchain

3.6.1 Introduction

Bitcoin, the very first cryptocurrency, has put blockchain technology in the spotlight due to its popularity and ease of use. Blockchain technology has its roots in the underlying structure of

the bitcoin cryptocurrency; it was first introduced to the online world through this medium, where it quickly gained attention and traction due to the high level of transparency it offered. Several disciplines as alternatives.

To put it briefly, blockchain is a distributed, immutable ledger that may be used to track assets and keep tabs on financial dealings inside a company network. Intangible assets include things like intellectual property, patents, copyrights, and branding, whereas physical assets include things like a house, car, cash, and land. Today, almost anything can be recorded and traded via a blockchain, making transactions cheaper and safer for all parties involved. Blockchain uses “blocks” to organize its data. Before being distributed across the network in individual blocks, all of the data that will be stored on the blockchain is first split into smaller components. A “Genesis Block” or “Block 0” is the first block in a blockchain. “Block 0” or “Block Gene-sis” In certain cases, the genesis block is hard-coded into software; when this occurs, the block is unique in that it does not include a connection to the preceding block. The Genesis block is unique in that it does not include a reference to the prior block (the Genesis block), which is often hardcoded into the program.

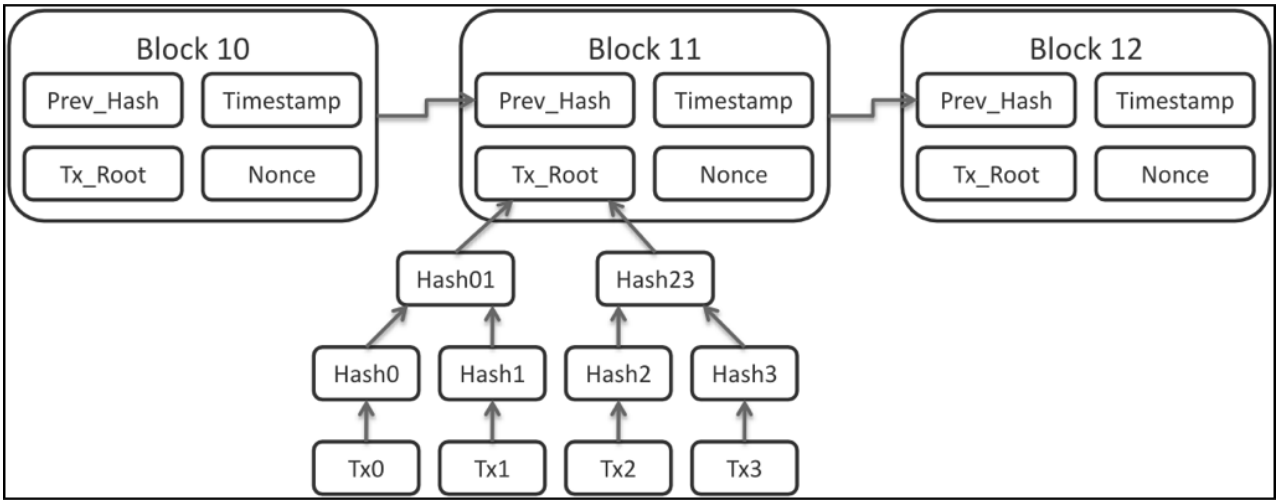


Figure 7 Hash Table

The ballot paper machine was a paper-based voting system used in India before to 2004. Therefore, the blockchain is the most practical alternative for the electronic voting platform, as it can address all the problems that plague the current system. There has been a lot of research into electronic voting, and many different implementations have been tried and deployed for short periods of time, where issues such user authentication, vote tempering, etc. have been

encountered. There are several government-run online resources, such as polling sites, informational networks, question and answer forums, etc. However, the same cannot be said for online elections, where each vote cast actually matters to the success or failure of a candidate. The most popular form of government in use today is a democratic form of government, and formal elections are a cornerstone of that form of government. When compared to the current voting system, the new electronic voting system will be simpler, more accessible to voters, and more secure than ever before. By expanding access to voting, these strategies help lower the barrier of entry for many statutes. This improves the experience for those who are sick, in the military, who live overseas, or who have travelled abroad for vacation, and gives it a fighting chance to endure long lines at checkpoints. Many people, it has been determined, did not vote because they were too lazy to do so, therefore the 26ecentralize voting method can fulfil its function here. Since everything else in the modern world is digital, the voting process has fallen behind. Voters between the ages of 18 and 30 represent a unique demographic, and attracting their support may be difficult.

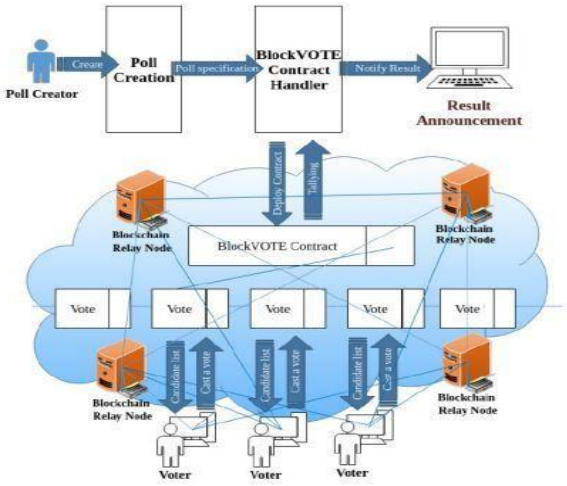


Figure 8 Architecture of E-Voting

3.6.2 Solidity

To automate financial dealings on the blockchain, developers turn to smart contracts written in Solidity, an object-oriented, high-level programming language. Developers on the Ethereum project came up with the language after it was introduced in 2014. The language's primary use case is in the development of smart contracts, both for the Ethereum blockchain and for usage with other blockchain implementations.

Solidity is comparable to JavaScript, a widely used computer language. It's similar to

JavaScript, but it's a somewhat different language. If you're familiar with JavaScript, you might find it simple to learn Solidity. The programming languages C++ and Python are also related to Solidity.

Solidity eliminates the requirement for binary code entry because it is a high-level language. It simplifies the process of writing computer programmes by allowing people to use a mix of letters and numbers that is more intuitive to them.

Inheritance, libraries, and sophisticated user-defined types are all supported in Solidity, which is statically typed. Static typing in Solidity requires the user to declare all variables. The compiler can ensure proper variable usage thanks to data types. The two main forms of data in Solidity are value types and reference types.When it comes to the EVM (Ethereum Virtual Machine), the primary distinction between value types and reference types is in how they are allocated to a variable and stored. While updating the value of one value type variable does not impact the other, updating the value of a reference type variable may result in the modified value being referenced by anybody.

• **How Does Solidity Work?**

The Ethereum ecosystem is attractive because it supports a wide variety of digital currencies and distributed applications. Ethereum's smart contracts enable the development of novel technologies for use by a wide range of industries and institutions.

The global expenditure on blockchain solutions annually is in the billions. Solidity is used to construct several of these solutions. To simplify and speed up interactions between parties in the business world and the rest of society, Solidity-based smart contracts can be used. This guarantees that all blockchain transactions are made by legitimate parties..

3.6.3 Smart Contract

Like any other contract, the details of an agreement are laid forth in a smart contract. Smart contracts, in contrast to traditional contracts, are put into action in the form of code on a blockchain platform like Ethereum. For industries as varied as lending, insurance, supply chain management, and gaming, smart contracts provide a way to implement complex peer-to-peer functionality.

• **How do smart contracts work?**

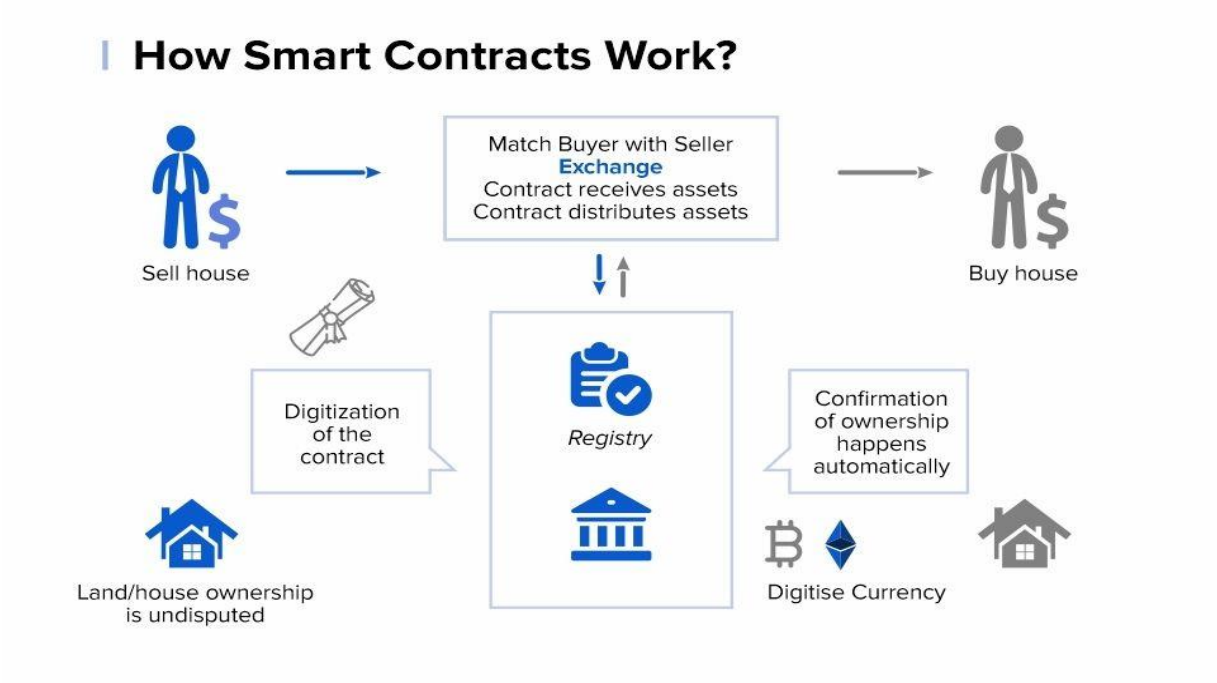


Figure 9 Smart Contract Working

There are several different programming languages used to create smart contracts, such as Solidity, Web Assembly, and Michelson. To ensure the correct operation of smart contracts on the Ethereum network, their source code is recorded in the distributed ledger and can be seen by anyone.In addition to the blockchain and transaction data, every computer on the network (a "node") holds a copy of all active smart contracts and their current state.

When a user deposits money into a smart contract, all of the nodes in the network run their code to determine the outcome and the subsequent flow of value. This is what makes it possible for users to conduct sophisticated financial transactions with unknown parties, while yet having the smart contract function autonomously and safely, without the need for a trusted third party.

A cost known as "gas" (so named because it funds the maintenance of the blockchain) must be paid in order to execute a smart contract on the Ethereum network.

3.6.4 Ethereum

Ethereum is a platform for decentralized application (app) and organization (org) development as well as asset (asset) storage, transaction (transaction), and communication (communication). With Ethereum, you may remain anonymous if you so want; you decide what is shared and what stays private. Ether, Ethereum's native coin, is accepted as

payment on the Ethereum platform. Here are some of Ethereum’s advantages.

A big, preexisting network. Ethereum's advantages include a’reliable network that has been put through its paces over the course of many years and billions of dollars’ worth of transactions. It has the largest blockchain and cryptocurrency ecosystem as well as a significant and dedicated user base through• Adaptable to a wide variety of settings.
When not being used for its own purposes, Ethereum may manage monetary transactions, s mart contracts, and data storage for other applications. Constant innovative work.
The vast Ethereum development community is always brainstorming ways to improve the l platform and build innovative applications.

The promise of Ethereum’s decentralized network is that it will eliminate the need for middlemen in several spheres of human activity, including the drafting and interpretation of contracts, the transfer of money, and the hosting of websites.

Ethereum Disadvantages:

- Increasingly high transaction costs. As Ethereum has gained in popularity, transaction fees have increased.
- Ethereum’s transaction fees, called as “gas,” may be extremely volatile and expensive. That’s fantastic if you’re a miner, but not so wonderful if you’re just trying to access the internet. Participants in an Ethereum transaction must pay the cost themselves, in contrast to Bitcoin’s system, which compensates individuals who verify transactions with tokens.
- Inflation in cryptocurrency is a possibility. Ethereum has a yearly cap of 18 million Ether, but there is no cap on the total amount of tokens that might ever be created. For investors, this may imply that Ethereum behaves more like dollars and doesn’t grow in value as quickly as Bitcoin, which has a fixed supply.
- • Developers have a steep learning curve. Ethereum’s learning curve can be steep for programmers making the switch from 29ecentraliz to 29ecentralized systems.

3.6.5 Metamask

Ethereum has risen as its popularity has grown.
In Ethereum, transaction fees are referred to as “gas,” and they have the potential to be both volatile and costly. If you’re a miner, that’s great news, but if you’re simply trying to go online, it’s not so great. In contrast to Bitcoin’s approach, which rewards those who verify

transactions with tokens, all Ethereum participants must bear the cost of the transaction individually.
Cryptocurrency inflation is a distinct possibility. While the maximum annual supply of Ether for Ethereum is 18 million, there is no limit on the potential size of the token supply. For those looking to invest, this might mean that the value of Ethereum is more stable than Bitcoin's, which has a fixed supply.
The learning curve for developers is high. Developers transitioning from centralized to decentralized systems may find Ethereum's learning curve challenging.

3.6.6 Truffle

The transaction expenses are getting to be too much. Increasing transaction costs are a direct result of Ethereum's rising profile.
For developers transitioning from 30ecentraliz to 30ecentralized systems, Ethereum can have a high learning curve..

3.6.7 Ganache

Ganache is a programme that helps us launch an Ethereum node on our local machine. The blockchain is a powerful tool because it can be used in every step of software development. Ganache enables us to launch, develop, and test all of our dApps in a secure and predictable environment while we set up our local blockchain.

.

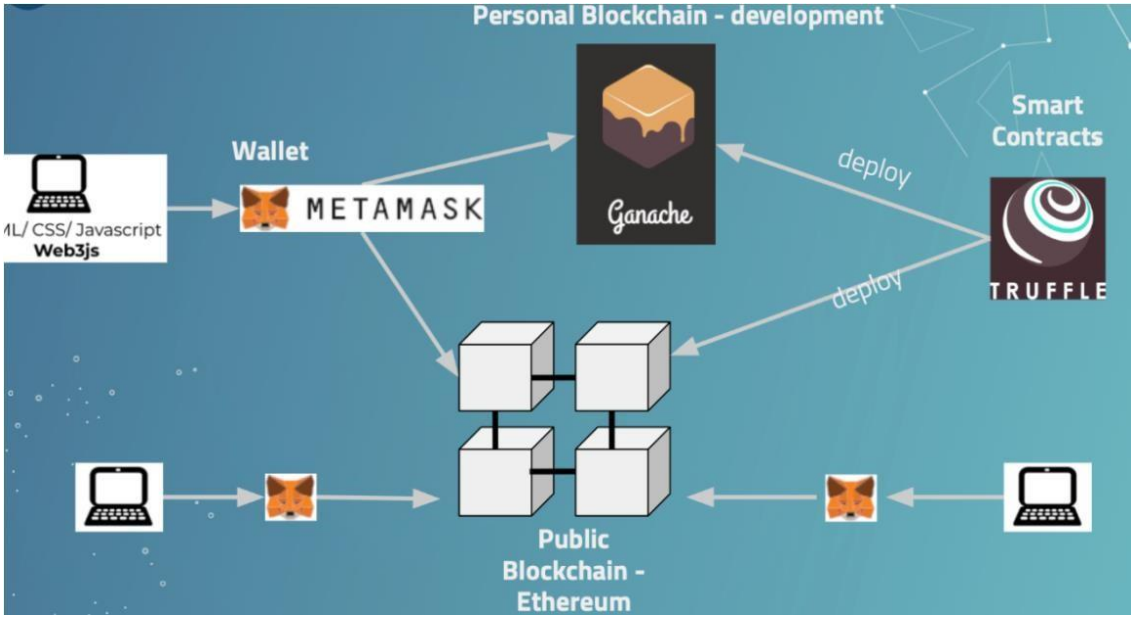


Figure 10 Blockchain Transaction Flow

3.7 Face Recognition

Here, we use facial recognition to verify users' identities. User authentication via facial recognition is required prior to voting for any candidate. There will be more confidence in the results of elections when voters can be assured that just their own faces are appearing on the ballots.

The simplest face recognition library in the world can be used with Python and the command line to perform recognition and manipulation of faces. Developed with dlib's state-of-the-art deep learning face recognition algorithm. Its performance on the Labelled Faces in the Wild benchmark is 99.38 percent accurate. The bundled face recognition command line program streamlines the process of identifying individuals in a large number of images.

3.7.1 Features

• **Find face**

Figure 11 Find Face

• **Find and manipulate facial features**

Get the locations and outlines of each person's eyes, nose, mouth and chin.

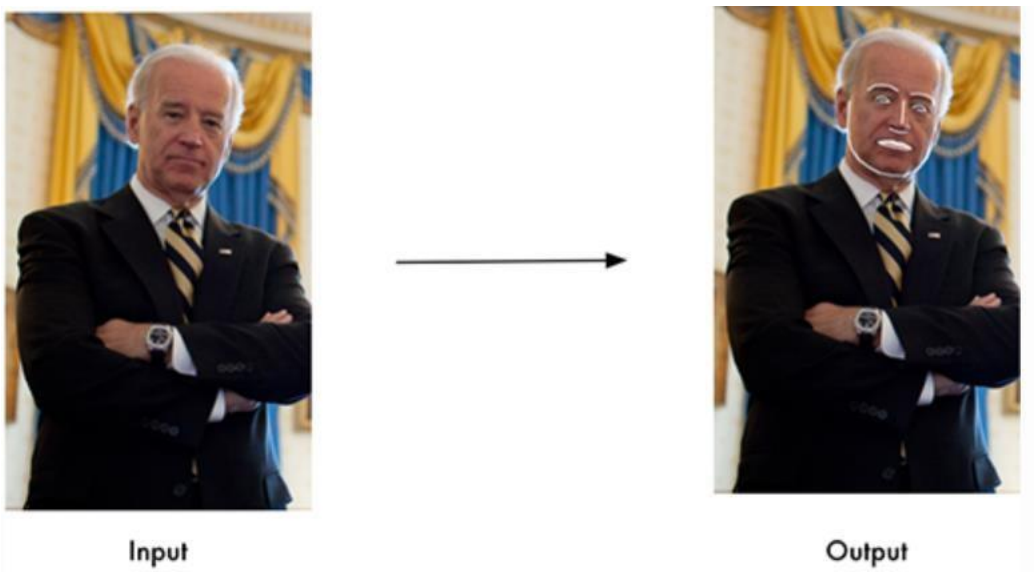


Figure 12 Extract Facial Feature

• **Identify faces in pictures**

Recognize who appears in each photo.

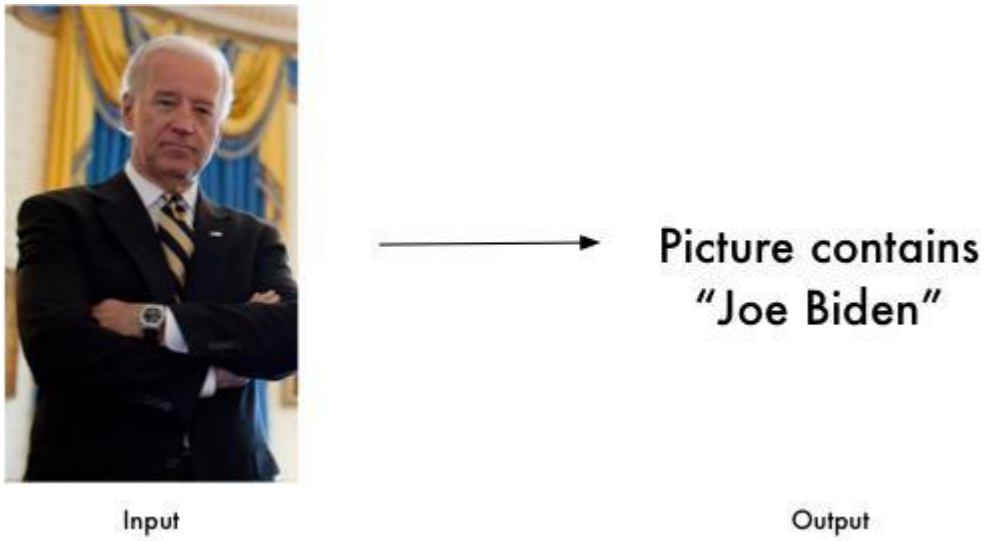


Figure 13 Identify Faces

3.7.2 Command-Line Interface

When you set up face recognition, you'll have access to a little command-line tool with the same name, which can be used to recognize faces in either a single photo or an entire album. You must first provide a folder in which one image represents each member of your current social group. It's important that each person in the shot has their own distinct image file, with names that accurately represent who they are. The files you want to tag must then be located in a separate folder.

By comparing the folder of known individuals against the folder (or single picture) of unknown people, the command face_recognition will tell you who is in each photo.

The finished product depicts each individual face as a single line. In the data, commas separate the filename from the name of the identified individual. We refer to a person whose face appears in a photo but who doesn't appear in the known_people folder as an unknown_person.

3.8 Timeline Chart

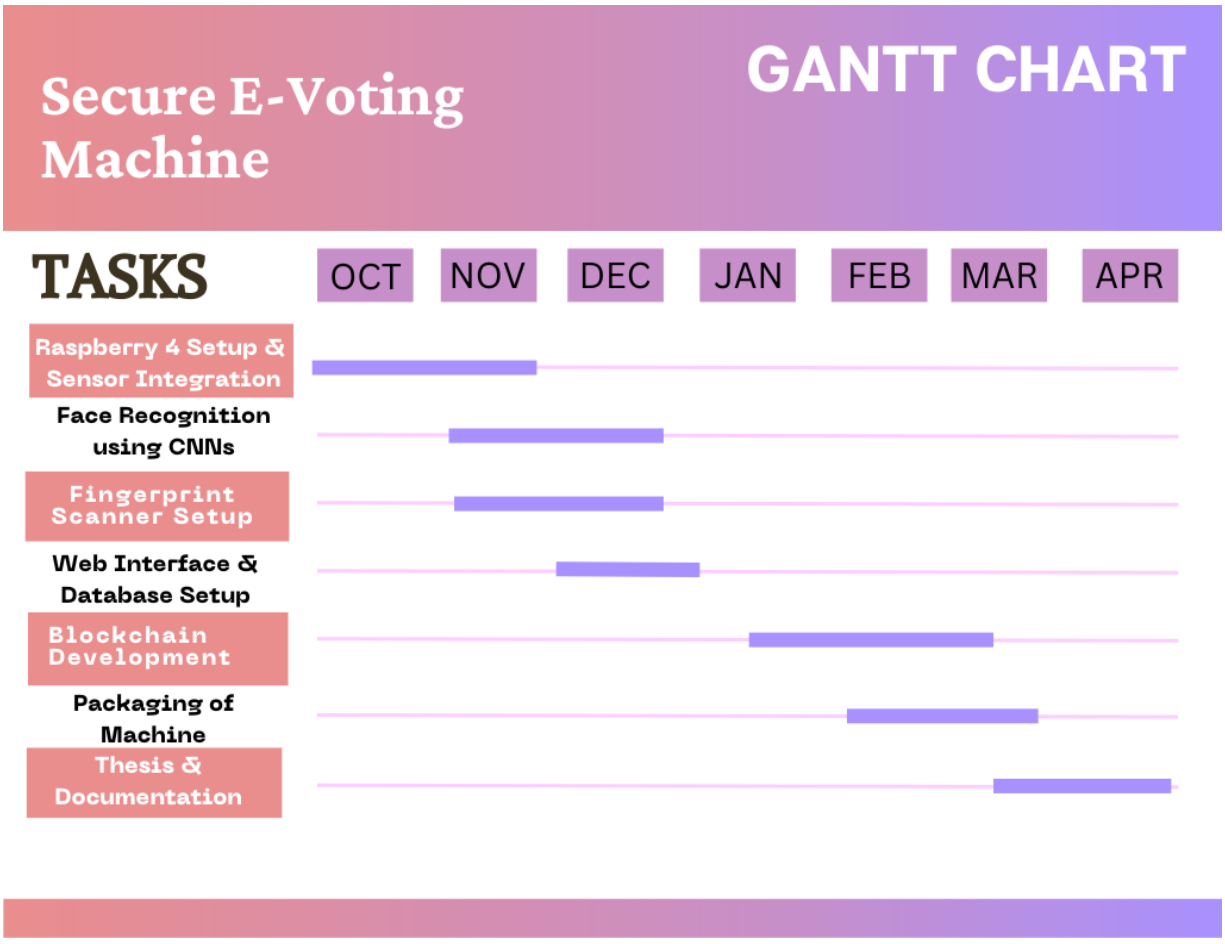


Figure 14 Project Timeline Chart

Chapter 4: Implementation and Testing

4.1 Software and Tools

4.1.1 Hardware Requirements

- Hardware that is **hosted locally.**

Hardware must be there until it is hosted to cloud servers and ready to pitch. After that anyone can use it through any smartphones or pc that has web browser inside.

The **Jetson Nano** is a small, powerful computer designed by Nvidia for use in embedded systems and artificial intelligence (AI) applications. It features an NVIDIA Maxwell GPU with 128 CUDA cores, a quad-core ARM A57 CPU, and 4GB of LPDDR4 memory.

The Jetson Nano is designed to run AI workloads, making it ideal for developing and prototyping AI applications such as object recognition, robotics, and autonomous vehicles. It is also capable of running high-performance computing workloads, making it a versatile platform for a wide range of applications.

The Jetson Nano comes with a range of software tools and libraries, including NVIDIA's JetPack SDK, which includes CUDA, cuDNN, TensorRT, and VisionWorks. These tools make it easy to develop and deploy AI applications on the Jetson Nano.

The Jetson Nano is small enough to fit into a variety of devices, including robots, drones, and other embedded systems. It also has a low power consumption, making it ideal for use in battery-powered applications.

4.1.2 Software Requirements

• React-js for the front end

• React is a UI-focused JavaScript library.

Single-page apps are constructed using React.

• The UI components we build with React may be used again and again.

• Stability at the Back End

To create smart contracts, Solidity is an object-oriented, high-level language. In the Ethereum blockchain, smart contracts are the governing software for how accounts are used.

• A Curly bracket language, Solidity was developed with the Ethereum Virtual Machine (EVM) in mind. It borrows ideas from Python and JavaScript in addition to C++. The section

on language effects provides further information about the languages that have influenced the development of Solidity.

• Solidity is statically typed, allowing for a wide variety of features, including inheritance, libraries, and sophisticated user-defined types.

• You can build voting systems, crowdfunding platforms, blind auctions, and multi-signature wallets with Solidity contracts.

• Contracts should be deployed using the most recent stable version of Solidity. Except in rare circumstances, security patches are only applied to the most recent release.

Additionally, both major and minor updates are consistently added. To reflect this rapid evolution, we presently use the version number 0.y.z.

• Extras: Web address, Web host, server, and online backup

The newest version of the front-end programming language, React-js, and the solidity language, which is required since the application runs on Blockchain technology, must already be loaded on the hardware.

4.1.3 Software requirements for our clients

- Windows 7 or higher OS
- Google chrome or any other safe browser

Client just need not to worry about anything just trust on over new innovation and head towards the transaction through any smartphone or pc that has web browser inside.

4.2 User Interface and Snapshots

4.2.1 Home page and Admin Login

Admin Login used for admin to Login in the System without email address and password admin or any other person can not login using this module as shown in Figure 15.

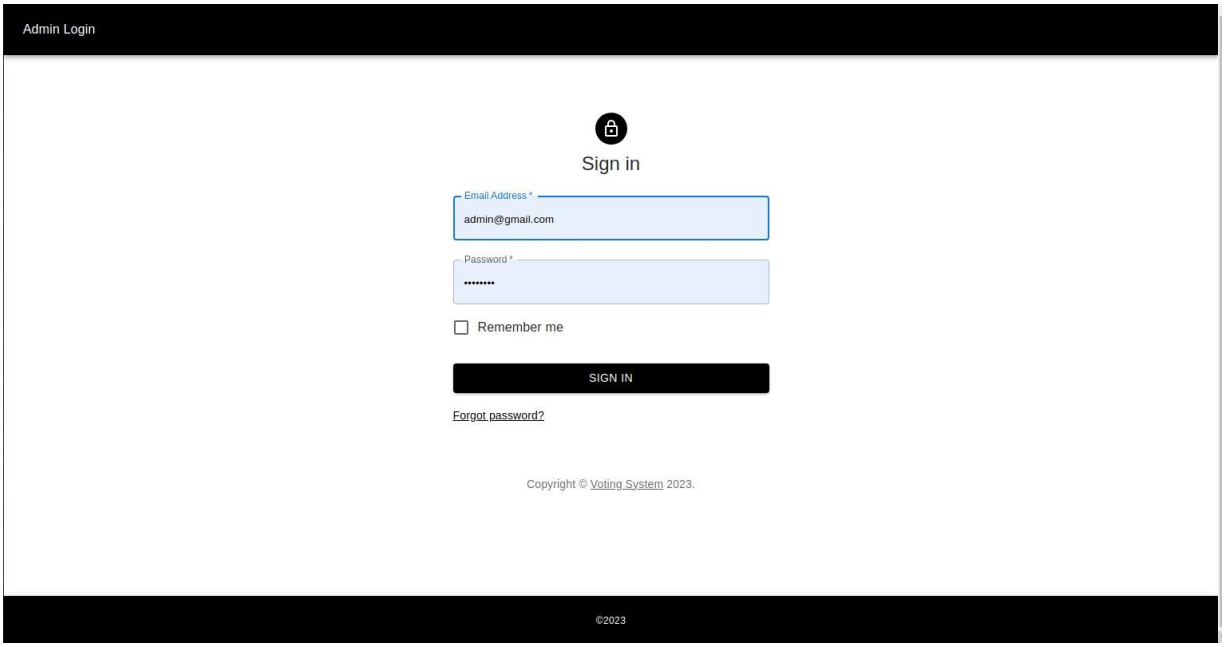


Figure 15 Admin Login

4.2.2 Admin Dashboard

Here Figure 20 shows Admin Dashboard where admin get all the information like total number of users, candidates and elections available in the system and also navigate to other modules like user candidate, election changing phase or showing result.

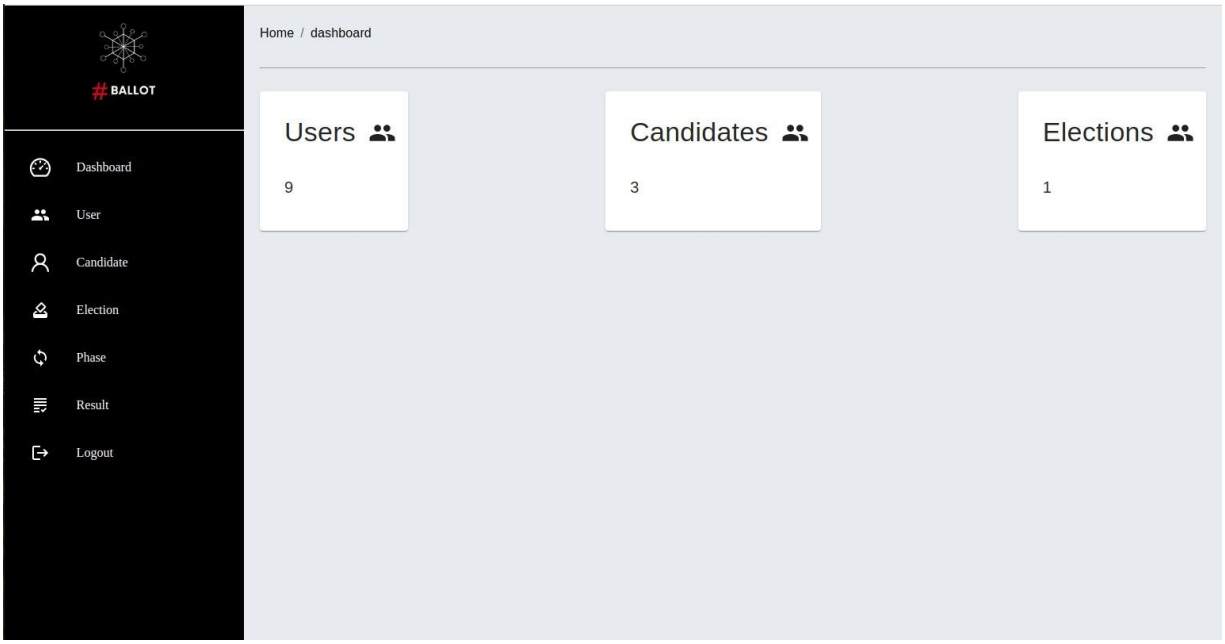


Figure 16 Admin Dashboard

4.2.3 View Users

Admin can view details of the users as shown in Figure 21. He can perform operations like edit users or delete user and add the user in the voting system.

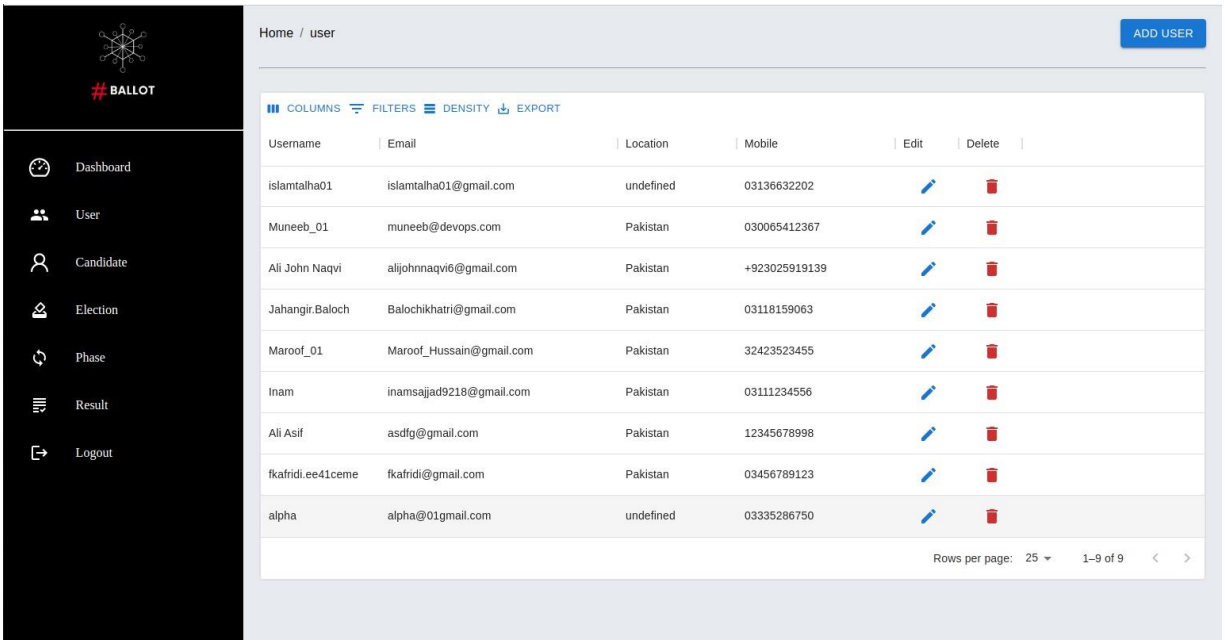


Figure 17 View Users

4.2.4 Add User

Admin can add user in the system using this gui where admin have to fill details like username, first name and other details after click on add user guy will get username and password in the e-mail which is entered in the given form.

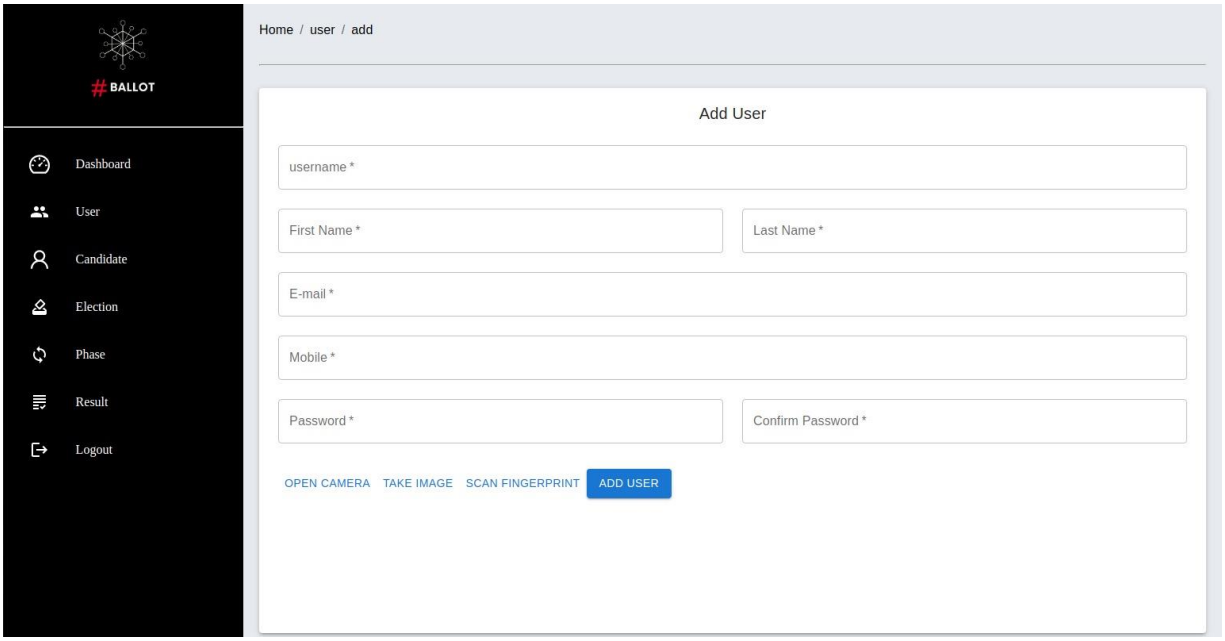
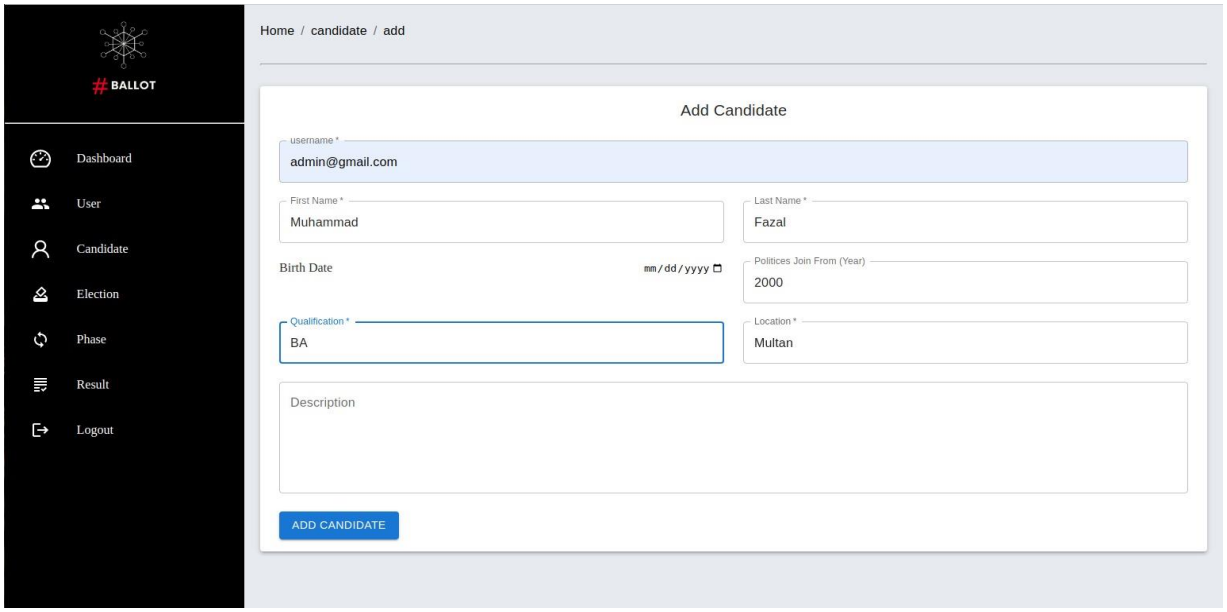


Figure 18 Add User

4.2.5 Add Candidate

Admin can add candidate and in the voting phase user will vote for this candidate.



.

Figure 19 Add Candidate

4.2.6 Add Election

Admin can add new election in the system with the unique election name and also add candidate from the available candidate with the dropdown menu of candidates.

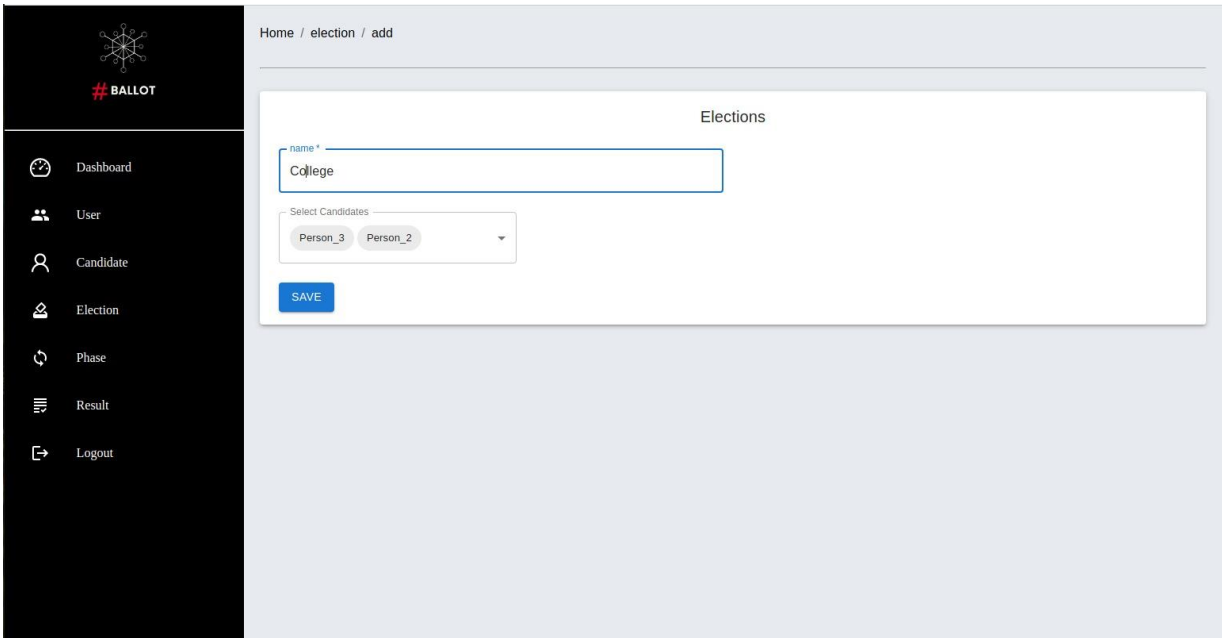


Figure 20 Add Election

4.2.7 Edit Phase

From this Page Admin can change the phase of election.

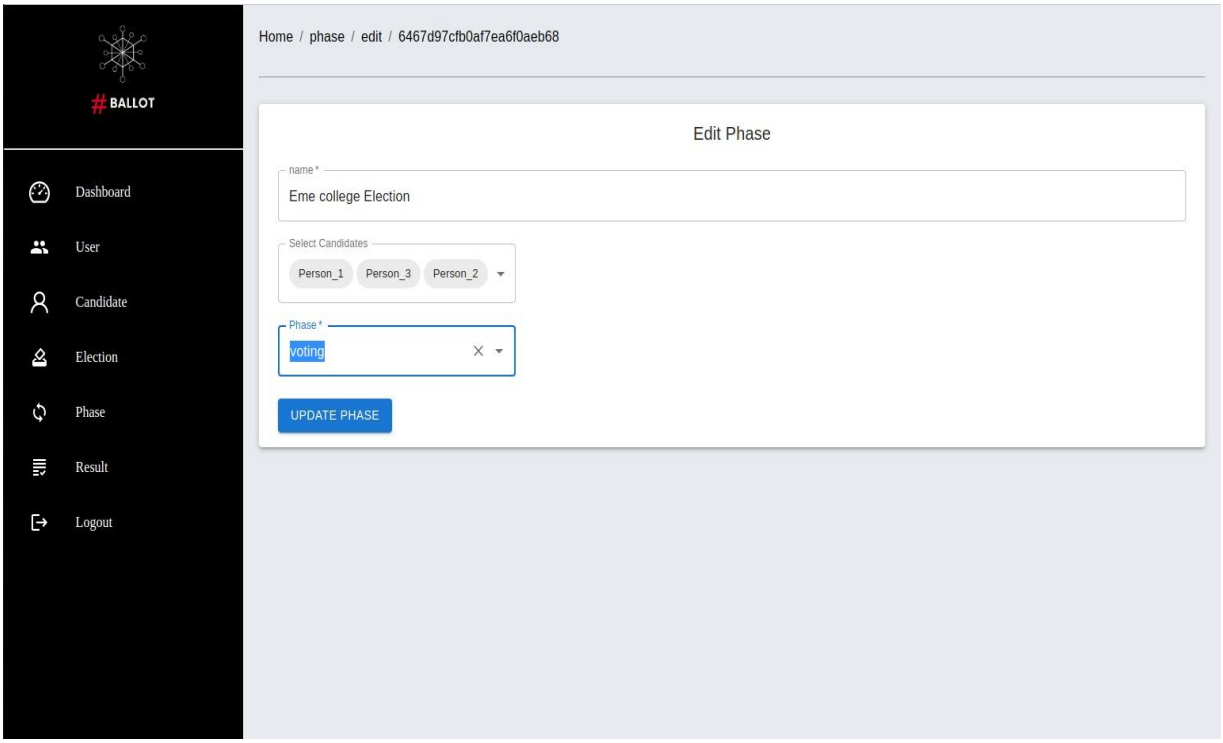


Figure 21 Edit Phase

4.2.8 View Elections

Here User can select election in which election user want to vote.

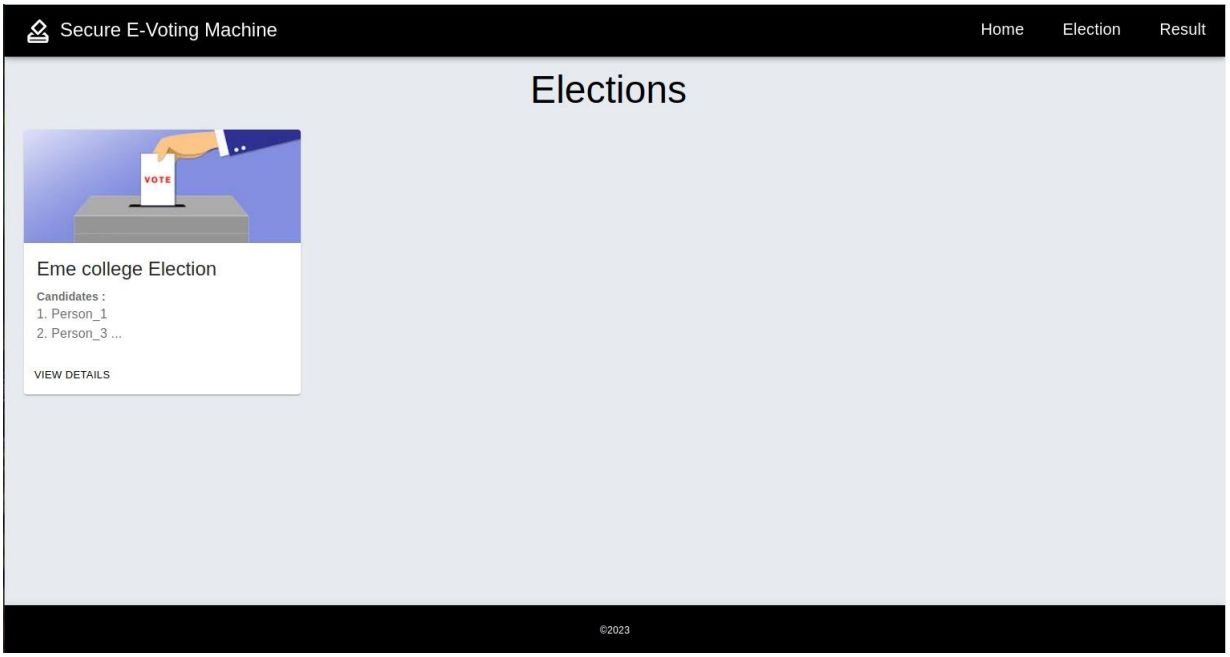


Figure 22 Elections

4.2.9 Candidate of Election

Here user can select candidate for voting and click on vote the python script will be execute and camera will be open in 30 seconds.

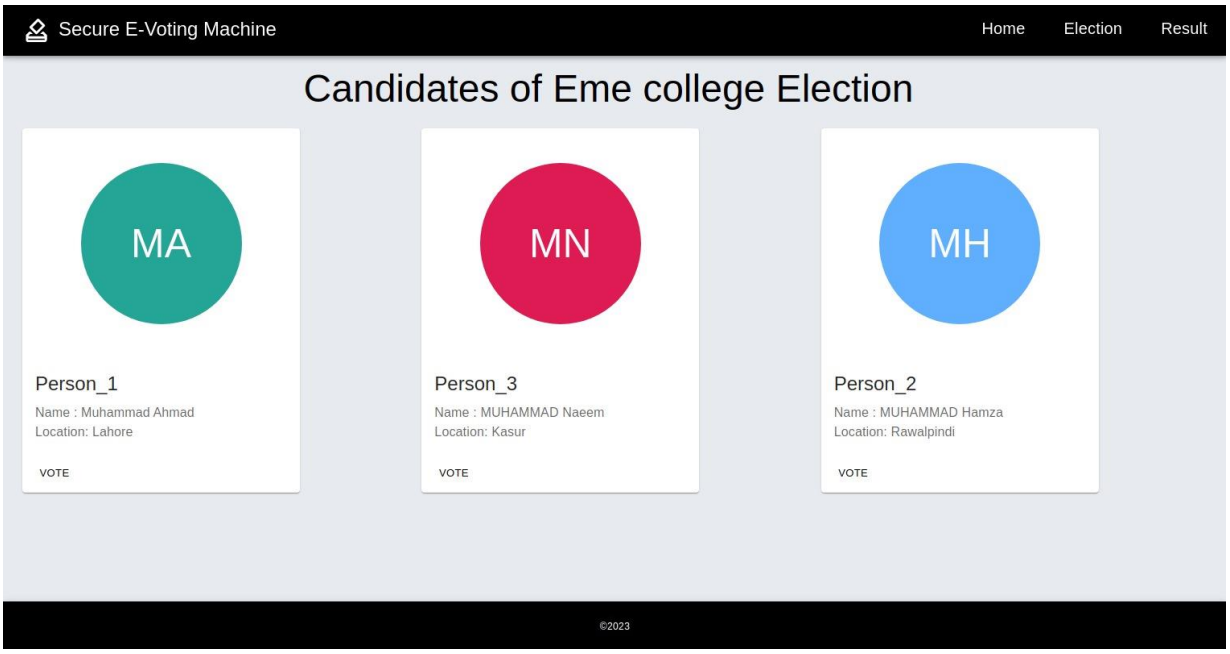


Figure 23 Candidates of Elections

4.2.10 Login User

User will be recognize using python script and the username will be shown in the username box automatically After entering right password metamask will be open for transaction.

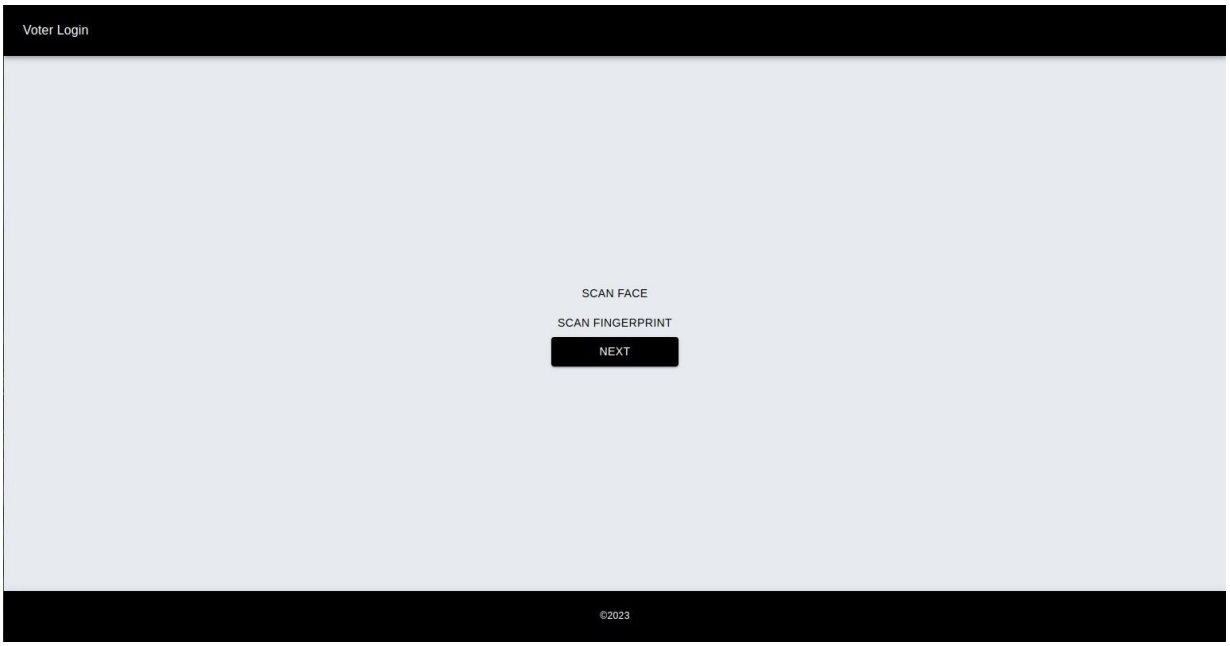


Figure 24 User Login Page

4.2.11 Voting Interface

Figure 25 Voting Interface

4.2.12 Metamask Transaction Details

Here Ethereum will be transfer from user account to candidate account using metamask After

confirming transaction user will get alert for successful transaction and also get email.

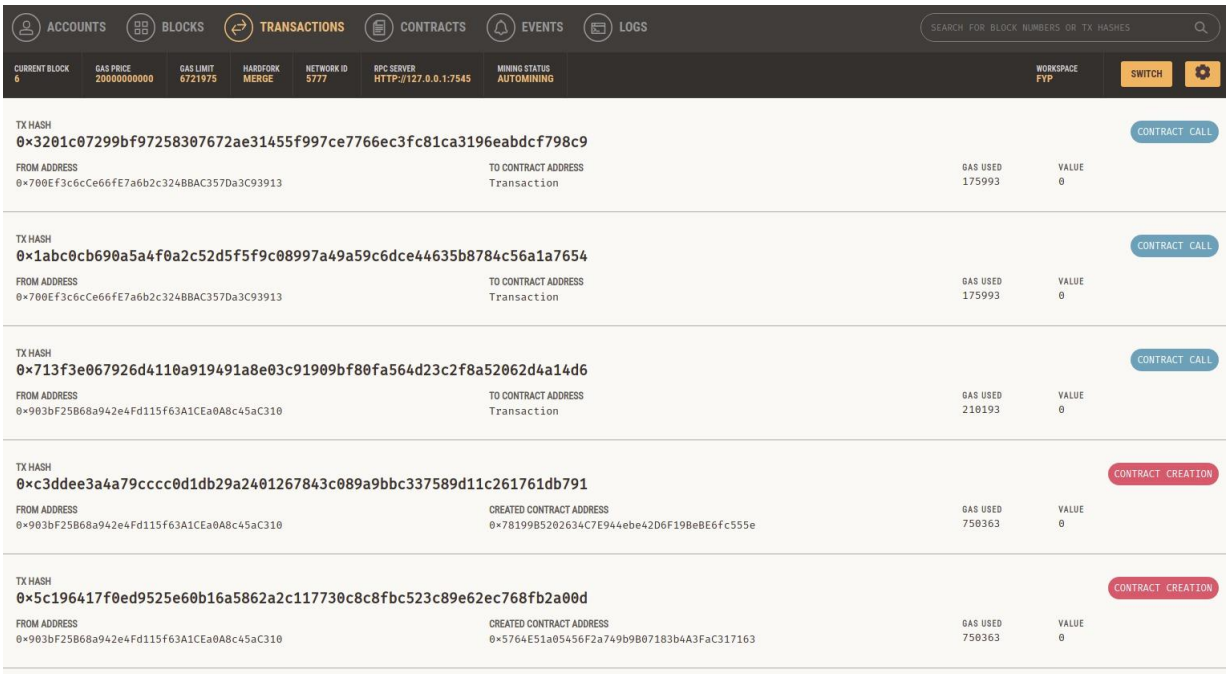


Figure 26 Transaction Details

4.2.13 Result of Elections

Here user can view all the election which phase is result and view details of the elections.

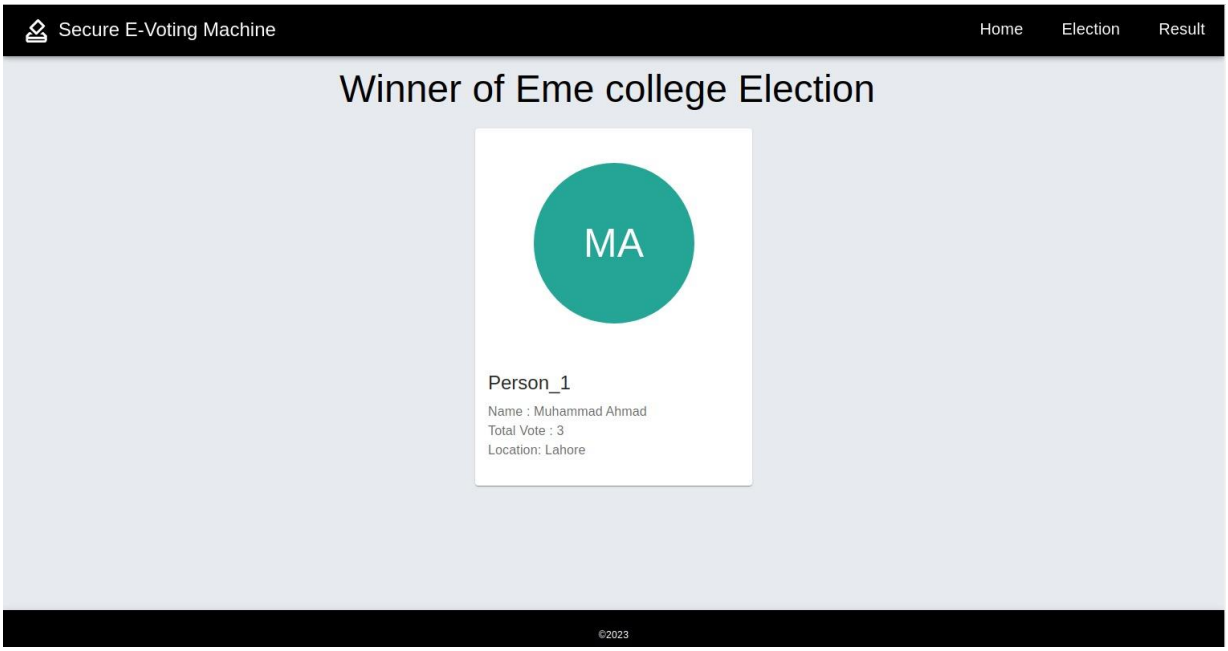


Figure 27 Result of Elections

4.2.14 Result of Candidates

Here user can view total vote of the candidate which election is chosen.

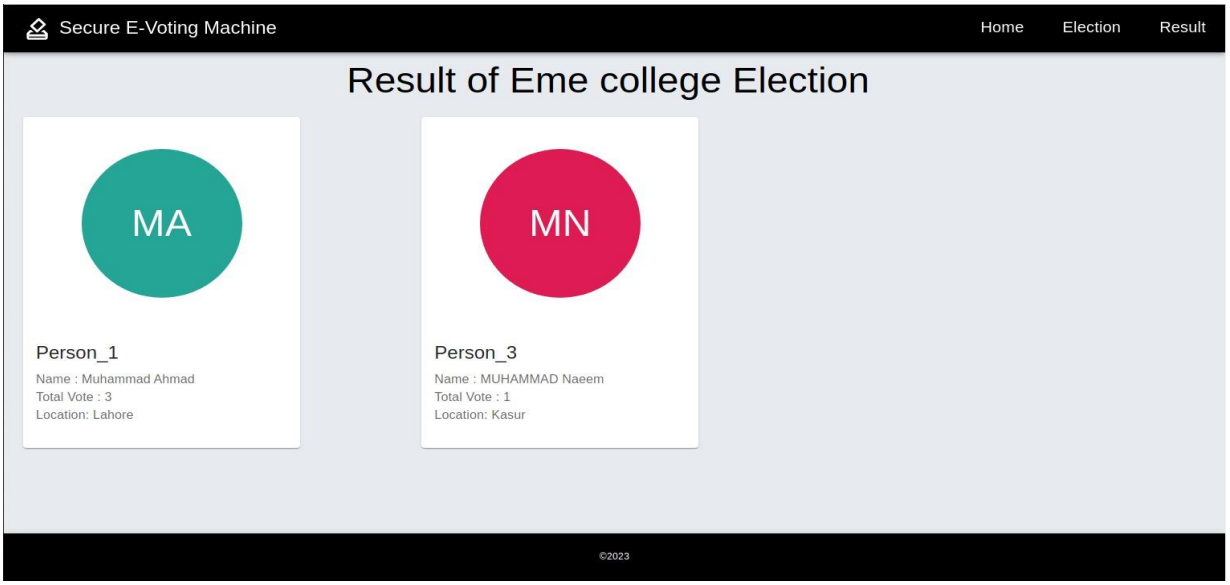


Figure 28 Candidate Result

4.2.15 Blockchain Account

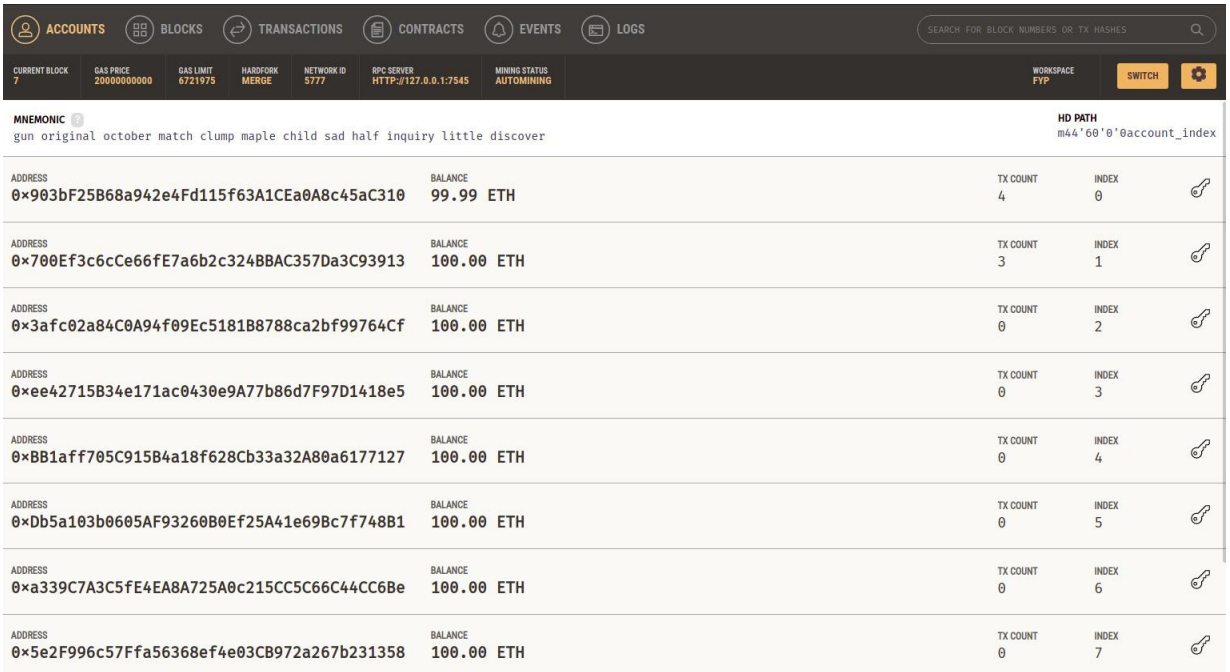


Figure 29 Blockchain account

4.2.16 Blockchain Block

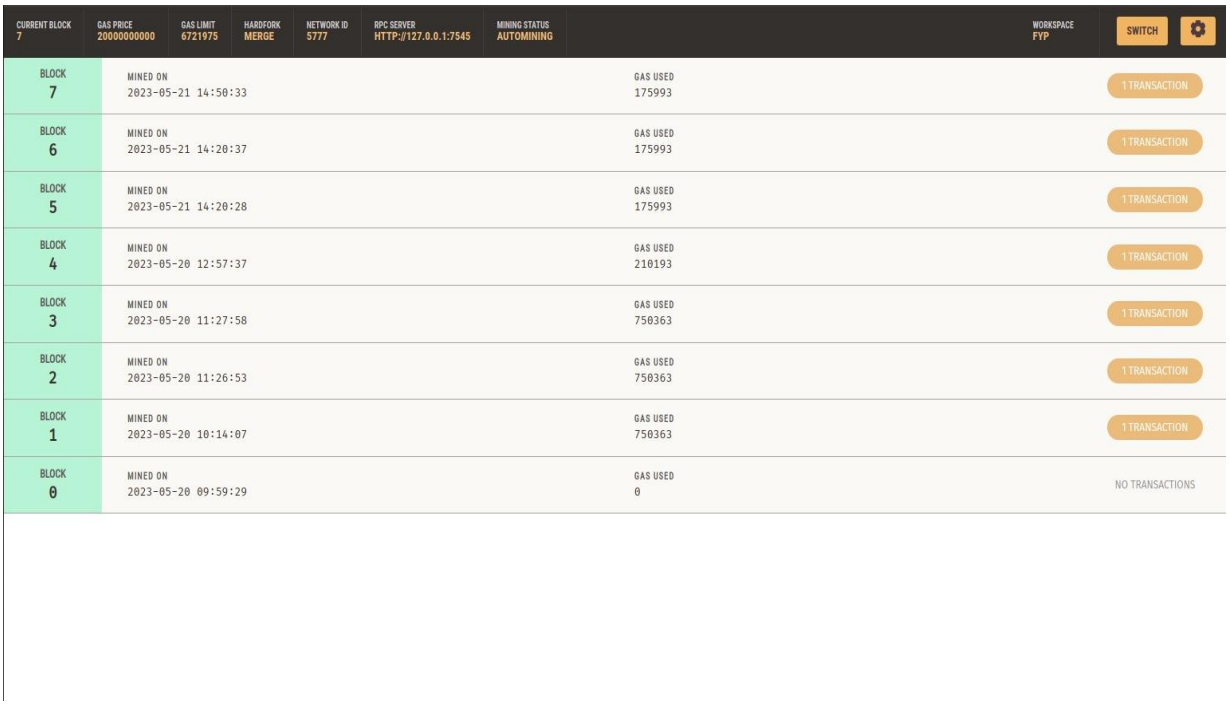


Figure 30 Blockchain Block

4.2.17 Transaction History

Figure 31 Transaction history

Chapter 5: Conclusion and Future work

5.1 Conclusion

In summary, this initiative eliminates the requirement for the user to bring any specialized equipment to the open air for writing. By making the most of our time and energy, we may effectively communicate our thoughts and ideas on paper.

Due to the use of a blockchain network and Two-Factor Authentication, the suggested machine is extremely safe.

Voting on a blockchain network is fast and can be done on a massive scale.

We built the front end in ReactJS and the back end in Flask (a python backend framework). Our Face Recognition system was created in Python with the help of OpenCV and dlib, and it communicates with a MYSQL database.

As things are, working online is a need. Mainly, teachers find it challenging to teach without writing, making online education more challenging. Our project is relevant in this context.

Once the project website is up on the server, instructors anywhere will have easy access to it, and those who want to do their work through pen and paper can do so with the help of a webcam. (For example, a maths teacher may use it to demonstrate an equation to their online class.)

To sum up, we can claim that we've developed a solution combining python libraries and OpenCV that will allow everyone to effectively communicate during online meetings, even if they don't have access to a keyboard.

5.2 Future work

Election Monitoring: Finally, election monitoring can be used to detect and prevent fraudulent activities. This can be done by having independent observers monitor the election process, using video surveillance, and conducting random audits to ensure the accuracy of the results.

ML Cyber Security:

Anomaly Detection: ML algorithms can be used to detect anomalous behavior in the election process, such as unusual patterns in voting behavior or attempts to manipulate the election results. By using ML to monitor the election process, it becomes possible to detect fraudulent activities and prevent them before they cause damage.

Predictive Analysis: ML algorithms can be used to predict potential cyber threats to the

election process. By analyzing historical data and identifying patterns in cyber-attacks, ML algorithms can predict future threats and help election officials take proactive measures to prevent them.

User Behavior Analytics: ML algorithms can analyze user behavior in election systems to detect unusual activity or attempts to manipulate the system. For example, ML algorithms can analyze user login patterns and detect suspicious login attempts or attempts to access sensitive data.

Natural Language Processing (NLP): NLP techniques can be used to analyze social media and detect potential threats to the election process. By analyzing social media activity, it becomes possible to detect fake news, disinformation campaigns, and other attempts to manipulate public opinion.

Fraud Detection: Finally, ML algorithms can be used to detect fraud in the election process. By analyzing voting patterns, it becomes possible to detect attempts to manipulate the election results or cast fraudulent votes.

Hash Balloting and User Privacy:

Hash Balloting: Hash balloting is a technique where a voter's identity is protected by generating a unique cryptographic hash value from their personal information, such as their voter ID or biometric data. This hash value serves as a pseudonymous identifier for the voter.
User Privacy: By using hash balloting and blockchain, user privacy can be preserved in the following ways:

a. Pseudonymous Identification: With hash balloting, voters are identified using cryptographic hashes, which do not reveal their actual identities. This protects their privacy and prevents the linkage of votes to specific individuals.

b. Data Encryption: Electronic voting systems can encrypt voter data to ensure its confidentiality during transmission and storage. Encryption techniques, such as symmetric or asymmetric encryption, can be employed to safeguard sensitive information.

c. Decentralization: Blockchain technology offers decentralization, where multiple nodes in the network maintain a copy of the ledger. This eliminates the need for a central authority that could potentially access or manipulate sensitive voter data.

So far, the project is effective and can be introduced at college or school level voting purposes that will ensure complete secrecy with no fraudulent behavior involvement.
As this system can be mainly used for college voting so it's part of face recognition can be used as an attendance system where we just must add the scanned student name into a file.
This system uses Ethereum coins for casting the votes so in future we can use Hyperledger (i.e., it doesn't use a cryptocurrency for transaction) for implementing blockchain so we can make this system free for people to cast votes.

Chapter 6: References

1. R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting", *Symmetry*, vol. 12, no. 8, pp. 1328, Aug. 2020.

2. 5. Onuklu, A. (2019), "Research on Blockchain: A Descriptive Survey of the Literature", Choi, J. and Ozkan, B. (Ed.) Disruptive Innovation in Business and Finance in the Digital World (International Finance Review, Vol. 20), Emerald Publishing Limited, pp. 131-148. DOI/10.1108/S1569-3767201

3. Zhang K, Zhang Z, Li Z, et al. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks [J]. IEEE Signal Processing Letters, 2016, 23(10):14991503.

4. Pranav KB, Manikandan J, " Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks", April 2020, ScienceDirect

5. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access* 2019, *7*, 24477–24488.

6. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. *IEEE Access* 2019, *7*, 115304–115316.

7. Ramya Govindaraj, P Kumaresan, K. Sree harshitha, " Online Voting System using Cloud," 24-25 Feb. 2020, IEEE

8. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* 2020, *8*, 21091–21116.

9. Yi, H. Securing e-voting based on blockchain in P2P network. *EURASIP J. Wirel. Commun. Netw.* 2019, *2019*, 137.

10. Torra, V. Random dictatorship for privacy-preserving social choice. *Int. J. Inf. Secur.* 2019, *19*, 537–543.

11. Alaya, B.; Laouamer, L.; Msilini, N. Homomorphic encryption systems statement: Trends and challenges. *Comput. Sci. Rev.* 2020, *36*, 100235.

12. Khan, K.M.; Arshad, J.; Khan, M.M. Investigating performance constraints for blockchain based secure e-voting system. *Future Gener. Comput.Syst.* 2020, *105*, 13–26.

13. **GITHUB REPO LINK:**
    - https://github.com/ageitgey/face_recognition
    - **Fingerprint**:

https://learn.adafruit.com/adafruit-optical-fingerprint-sensor/circuitpython

- **Face ID**: https://pyimagesearch.com/2018/06/18/face-recognition-with-opencv-python- and-deep-learning/
- **LCD Setup**:
    - http://www.lcdwiki.com/5inch_HDMI_Display

Plagrism

ORIGINALITY REPORT

12%	8%	3%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Higher Education Commission Pakistan Student Paper	2%
2	ijisrt.com Internet Source	1%
3	Submitted to University of East London Student Paper	1%
4	turkiye.un.org Internet Source	1%
5	Submitted to Swinburne University of Technology Student Paper	<1%
6	Submitted to Universiti Malaysia Perlis Student Paper	<1%
7	Submitted to Federation University Student Paper	<1%
8	Submitted to Cranfield University Student Paper	<1%

9	Submitted to Universidad Anahuac México Sur Student Paper	<1%
10	github.com Internet Source	<1%
11	Submitted to Muscat College Student Paper	<1%
12	Submitted to Informatics Education Limited Student Paper	<1%
13	www.termpaperwarehouse.com Internet Source	<1%
14	Submitted to WorldQuant University Student Paper	<1%
15	fics.nust.edu.pk Internet Source	<1%
16	www.itu.int Internet Source	<1%
17	Submitted to University of Portsmouth Student Paper	<1%
18	d-nb.info Internet Source	<1%
19	umpir.ump.edu.my Internet Source	<1%
20	uwspace.uwaterloo.ca	

		<1 %
21	link.springer.com Internet Source	<1 %
22	www.coursehero.com Internet Source	<1 %
23	www.opensourcelisting.com Internet Source	<1 %
24	Submitted to Coventry University Student Paper	<1 %
25	curatecoin.com Internet Source	<1 %
26	www.mdpi.com Internet Source	<1 %
27	Submitted to University of Bedfordshire Student Paper	<1 %
28	Submitted to University of New Haven Student Paper	<1 %
29	Rahimi, . "The Microsoft .NET Platform", Distributed Database Management Systems A Practical Approach, 2010. Publication	<1 %
30	"Adaptive packet processing on CPU-GPU heterogeneous platforms", Institution of Engineering and Technology (IET), 2019	<1 %

31	Amitabh Bhargava, Ajay Rana, Deepshikha Bhargava. "Blockchain based digital voting system: A secure and decentralized electoral process", 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), 2022 Publication	<1 %
32	Submitted to British University in Egypt Student Paper	<1 %
33	brasilbrownies.com.br Internet Source	<1 %
34	xml.jips-k.org Internet Source	<1 %
35	"IOT with Smart Systems", Springer Science and Business Media LLC, 2023 Publication	<1 %
36	Submitted to Ghana Technology University College Student Paper	<1 %
37	Submitted to University of Greenwich Student Paper	<1 %
38	qualitywalagyan.com Internet Source	<1 %
39	canadafreepress.com Internet Source	<1 %
40	hdl.handle.net Internet Source	<1 %
41	openaccess.city.ac.uk Internet Source	<1 %
42	staging.ethereum.org Internet Source	<1 %
43	Harry Blutstein. "Chapter 3193 Globalization and World Trade Organization", Springer Science and Business Media LLC, 2022 Publication	<1 %