DEVELOPMENT OF AN ELECTRONIC FACIAL RECOGNITION VOTING SYSTEM USING BLOCKCHAIN TECHNOLOGY

BY

ADEKUNLE ESTHER TEMITOPE
(SSE/017/18609)

A PROJECT SUBMITTED

TO

COMPUTER SCIENCE PROGRAM,

COLLEGE OF COMPUTING AND COMMUNICATION STUDIES,

BOWEN UNIVERSITY, IWO OSUN STATE NIGERIA.

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD DEGREE OF BACHELOR OF SCIENCE (B.Sc.) IN COMPUTER SCIENCE

AUGUST 2021

CERTIFICATION

This is to certify that this project, Electronic facial recognnition voting system using Blockchain Technology was carried out by Adekunle Esther Temitope (Matriculation Number: SSE/017/18609) of the Computer Science programme under my supervision

…………………………………	…………………………………
Dr. A.O. Ibitoye	Date
(Supervisor)	

…………………………………	…………………………………
Dr A.O. Akinwunmi	Date
(Programme Coordinator)	

DEDICATION

I dedicate this project to GOD Almighty, for His grace, love, provision, mercy, guidance, and care granted to me throughout this research work and for the strength to scale through every challenge faced during the period of this project work.

Finally, I dedicate this to my Parents, Mr Adelodun Adekunle, and Mrs. Victoria Adekunle and my loves, Esther, Adeks and Deksy for always being there as a source of inspiration, correction, and encouragement.

ACKNOWLEDGMENT

My sincere gratitude goes to the Almighty God, for being my Sustainer, Helper and for guiding me successfully towards the completion of this research work.

I want to appreciate my project supervisor, Dr. Ayodeji O. Ibitoye, for his patience and fatherly love to me towards the successful completion of my project. I am grateful to the Provost, Dr M.O. Oyelami, Programme Coordinator, Computer Science, Dr. A.O. Akinwunmi and to all my lecturers, Prof. O.O. Olabode Dr. D.O. Lanloye, Dr. R.F. Famutimi, Dr. Mrs. O.N. Emuoyibofarhe, Mr. B.P. Ayaniyi, Dr. E.K. Olatunji, Dr. T.O. Olorunfemi, Dr. Segun Adebayo, Dr. A.O. Abiodun, Dr. H.O. Aworinde, Dr. O.M. Awoniran, Mr. A. Adeyemo and Mrs. Olaniran for their impactful knowledge.

I wish to express my profound gratitude to my dear parents, Mr. and Mrs. Adekunle who kept praying and pushing, providing financial means to support me, I also want to appreciate my siblings, Akinade, Adedotun, Adekemi and David for always supporting and encouraging me during the course of this research.

I am grateful to my friends, Opeloyeru Olayinka, Elegbeleye Temitayo, Nwandu Yadirichi, Jegede Timilehin, Olutunmbi Blessing, Adeksydeks and for their unlimited support, love and patience throughout this project.

Finally, I would like to express my sincere gratitude to everyone who supported me in the course of writing this project.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Voting is a very important issue which can be beneficial in term of choosing the right leader in an election. However, elections are surrounded with voting issues like manipulation of results, it is time consuming. Moreover, a voters details can be used to login and vote by another person.

In this project, a decentralized electronic voting system based on Blockchain Technology and an integrated Facial Recognition to improve the security of the system. Blockchain is a distributed database in which data are shared with the participant of the node and each participant holds the same copy of the data. Blockchain has properties like distributed, data integrity etc. Smart contract is used to create the voting process and is deployed on the ethereum network (Blockchain).

The project results in a transparent, non-editable and independently verifiable procedure that discards all the intended fraudulent activities occurring during the election process by removing the participation of a middleman and enabling voters’ right during the election.

In conclusion, the project encourages participation from citizens using Blockchain technology and verification of faces during election which has proved to be more convenient for counting votes and ensuring the process goes smoothly than the traditional methods. Both transparency and coercion are obtained at the same time.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF STUDY

Decisions must be made amongst various possibilities in today's democracy, which includes people with conflicting and inconsistent viewpoints. This occurs in the Commercial world, Educational world, Social organizations, and, most notably, in Government. Elections are crucial component of a democratic system because the general public are allowed to express their opinions through voting, yet citizens in their country lack confidence in their electoral process, which is a huge source of concern for the government (Khan et al., 2018).

For Instance, A democratic election in a country or state requires a high level of security. On the other hand, because voting is a formal statement of an individual's or group's opinion or decision, notably in an election (Figure 1.1). It is a major event that affects a nation's fate, it is critical to implement proper and stringent security measures to ensure free and fair voting.

For Instance, In Nigeria, different election categories takes place at the federal level, a head of state (the President of Nigeria) and a legislature (the National Assembly) (Wikipedia, 2021). The president is chosen by the general public(Wikipedia, 2021). There are two chambers in the National Assembly. The House of Representatives who has 360 members and the Senate who has 109 senators elected for a four-year tenure (Goitom, 2012). A presidential candidate must earn a majority of the vote and more than 25% of the vote in at least 24 of Nigeria's 36 states (Wikipedia, 2021).

Figure 1.1: Ongoing Voting

(Source: (Ben et al., 2019))

E-voting is being explored extensively, and a number of implementations have been developed and even used in the past. Only a few implementations, however, have proven to be stable and are still in use. Furthermore, in democratic nations, a strong constituent approach with openness and privacy may be highly regarded. There are five types of voting machines used:

1. Hand-counted paper ballots are marked by hand, usually with an X next to a candidate to indicate the voter's decision (Figure 1.2). The ballots are then manually counted in the area where they were cast. Hand-counted paper ballots are no longer often used in the United States; nevertheless, they are more popular in other nations, particularly those with only one race on the ballot at a time (VerifiedVoting, 2020).

Figure 1.2: Paper ballots.

Source: (*Voting Equipment – Verified Voting*, 2020)

2. Mechanical lever voting system, first used in the 1890s, he or she pulls a huge lever that pulls a curtain around the voter, assuring privacy (Figure 1.3). When a voter is completed, he or she pulls the huge lever once again, causing the counters connected with his or her choices to be incremented by one and the system to be ready for the next voter (VerifiedVoting, 2020). Votes are counted at the conclusion of Election Day by opening the machine and reading the numbers on the counters connected with each candidate.

Figure 1.3: A mechanical voting system

Source: (*Voting Machines - Elections - Ballots - Politics - The New York Times*, 2008)

3. Punch-card voting devices developed in the 1960s used modified Hollerith cards to register votes (VerifiedVoting, 2020). When a voter wants to vote for a candidate, he or she uses a stylus to remove a chad (the pre-scored piece of paper) and punch a hole in the card with the candidate's number (Figure 1.4). When the voter is finished, he or she deposits the ballot card in a ballot box. The ballots are counted using a card reader at the end of Election Day, usually in the central election office.

Figure 1.4: Punch-card voting system

Source: (*Early Card Punch Machines*, 2021)

4. Direct-Recording Electronic (DRE) machines came into use in the 1970s. The earliest DREs were electrical versions of mechanical levers with push buttons and electrical storage devices (VerifiedVoting, 2020). Nowadays, DREs are now simply portable computers that have been set up to display ballot options and then electronically record votes (Figure 1.5). On a computer touch screen, ballot options are increasingly available. Although some systems rely on push buttons, most modern DREs allow the voter to indicate a vote by pressing on the touch screen (Ndem, 2018). DREs are increasingly include a paper record known as a Voter-Verified (or Verifiable) Paper Audit Trail (VVPAT) that may be used to audit or recount an election (Ndem, 2018).

Figure 1.5: A direct recording electronic device

Source: (Ndem, 2018)

5. I-voting known as internet voting; There is no more convenient place to vote than from the comfort of one's own home, regardless of how effectively polling booths are constructed and placed. By making voting as simple as entering into a website, checking a few boxes on a form, and hitting the "Vote" button, voter turnout and thus the general legitimacy of the results are likely to rise dramatically (VerifiedVoting, 2020) (Figure 1.6). Electronic ballots can be counted and tabulated faster and more easily than traditional paper ballots (Miller, 2020).

Figure 1.6: Internet Voting

Source: (Miller, 2020)

According to the facts and research presented above, while the I-voting system has solved the constraints of other types of voting systems, security is a different story. The most critical difficulty for the I-voting system is security, which is one of the public's interest in blockchain technology originated for a variety of reasons. In this scenario, Blockchain is the most widely used technology suited for both "transparency" and "security," as a result the proposed system's concept (Sharma et al., 2019).

Blockchain technology, which shone like a star after the broad acceptance of Bitcoin (Nakamoto, 2009), the world's first cryptocurrency, has become a hot topic in today's package world. Blockchain was initially just used for financial transactions and commerce, but studies have begun to suggest that it will be used in other areas over time as a result of the system's high degree of transparency(Sharma et al., 2019).

For example, in Bitcoin, because the wallets are dispersed widely, the total number of currencies and instant group activity volume around the world can be tracked instantly and clearly. On this P2P-based system, there is no need for a central authority to authorize or complete the assignment. As a result, not only money transactions but also all forms of structural data will be unbroken throughout this dispersed chain, and the system will be kept secure through the use of cryptographic methods. Ethereum coin (Ether), another cryptocurrency with useful development environments that debuted a few years after Bitcoin, distinguishes the blockchain in a very real sense, indicating that this technology will create a package that will retain information that is structured as described above (Nakamoto, 2009). Package programs enforced by smart contracts are written into the blockchain and are immutable; once written, they cannot be (illegally) deleted or changed. As a result, they will always function properly, autonomously and transparently, regardless of external stimuli. As previously said, the blockchain innovation handles a number of challenges related to e-voting thanks to its unique distributed and safe concept but anyone with the login details can access the network with an internet connection which gave rise to my statement problem.

1.2 STATEMENT OF PROBLEM.

The existing system of voting using Blockchain is faced with the problem of impersonation where someone can vote illegally with the details of another voter.

1.3 AIM

The aim of this project is to design an electronic facial recognition voting system using Blockchain Technology.

1.4 OBJECTIVES

1. To create a smart contract that is deployed on the ethereum network.
2. To develop a secure database for storing voters face ID's.
3. To integrate a Facial Recognition software for verification of voters.

1.5 METHODOLOGY

i. Extensive reviews of related works and existing processes will be carried out by reading published materials, newspapers and internet browsing. The information collected will be examined to obtain the necessary and important information necessary for the system.

ii. A diagram software called Diagrams.net will be used for flowcharts, use case diagram and architectural diagram.

iii. It will also be implemented as a mobile application, the system will be developed using Flutter for front-end, Node JS for backend of the application and integrating Kairos as the facial recognition software.

iv. The test would involve the ease of use, feasibility, and capabilities, overall performance, and satisfaction.

1.6 JUSTIFICATION OF STUDY

The project's benefits are listed below, in light of the rapid growth of computer technology in nearly all domains of operation and its usage in relation to information management.

1. It will give the Electoral Commission a way to organize elections that are less expensive and more fair, as well as cut down on the time spent collating and releasing results.
2. Data and information are safeguarded by the secure and flexible database management system, ensuring credible elections.
3. It will help to lessen the workload throughout the election process.
4. It allows people to vote from the comfort of their own homes because it integrates remote voting.
5. It will help to remove illegitimate votes and reduce election violence by counting votes as soon as they are cast.

1.7 SCOPE OF STUDY

This project is focused on developing an Electronic facial recognition voting system using blockchain to boost the trust of citizens in the election process.

1.8 LIMITATIONS OF STUDY

1. Governments and stakeholders must overcome three major challenges of blockchain's complexity, lack of broadband connectivity, and lack of digital user skills may hinder its adoption by the general public.
2. Using facial recognition software, a slight change in camera angles or personal appearances can cause errors and not all smart phones are 100% efficient.

1.9 ORGANIZATION OF PROJECT

i. **Chapter One**

Chapter one is the introduction that covers the basics of voting and elections. It goes further to explain the background of study, Aim and Objectives, Statement of problem, Justification, Scope, Methodology Limitations and Organization of project.

ii. **Chapter Two**

Chapter two describes the summary of literatures reviewed on the research and related works. It also describes existing systems, their implementation, critique, and literature reviews, as well as pointing out gaps in the available literature.

iii. **Chapter Three**

Chapter three describes extensively on the methodology, system analysis and the design of the system model.

iv. **Chapter Four**

In chapter four, we discussed about the procedures performed and approaches used for the project’s actual implementation. We can see tests being run to check that the project is running smoothly, as well as the results and their importance.

v. **Chapter Five**

In Chapter five, we wrap up the project and make some key recommendations for the product's best performance. We also make suggestions for how to improve, enhance, and optimize our current work**.**

CHAPTER TWO

LITERATURE REVIEW

This chapter gives insight into various articles, books, journals and other sources relevant to electronic voting system using blockchain and facial recognition. It also describes the relevant terms associated with Blockchain technology and Facial recognition. This leads to a deeper understanding of the problem and a knowledge of the value of the projects.

A storage needed to store information about the user that can be accessed anytime is a database. A database is electronic and the collection of data or information that is organized specially for quick search and retrieval by a computer.

2.1 DATABASE TECHNOLOGIES

Data collection, storage, aggregation, manipulation, distribution, and administration are at the heart of every well-designed system. Data are raw facts. The word raw indicates that the fact are not yet processed to make meaning. Information are processed data and it is meaningful to the user. The two main techniques for storing data in computers are: file system and database.

A file program is a system that controls how and where data is saved, retrieved, and managed on a storage disk, generally a hard disk drive (HDD). It compresses and organizes files into directories(Techopedia, 2016).

A well-structured system, known as a database, is critical when it comes to an organization's data, such as personnel information, financial records, and so on. Database is a collection of structured data that is regularly saved in a computer in a secure manner. Most of the time, a database management system is in charge of the database (DBMS). A database system is frequently reduced to merely database, which contains the data, database management system, and applications (ORACLE, 2015).

2.1.1 Database Management System

A database management system (DBMS) is a piece of software that allows you to use a database. The basic goal of a database management system (DBMS) is to provide a straightforward and efficient means of generating, updating, storing, and retrieving data from a database. It enables end users and application programmers to share data, and it enables data to be shared among multiple applications. Some examples of popular database software or DBMSs include MySQL, Microsoft Access, Microsoft SQL Server, FileMaker Pro, Oracle Database, and dBASE (ORACLE, 2015).

2.1.2 Components of DBMS

The major components of a database management system (Figure 2.1) are;-

i. Hardware

   This consists of a set of physical electronic devices such as I/O devices, storage devices and many more. It also provides an interface between computers and real-world systems (Vaishnavi, 2020).

ii. Software

   Software is the main component of a DBMS. It is the set of programs that are used to control and manage the overall Database (Vaishnavi, 2020). It also includes the DBMS software itself. The Operating System, the network software being used to share the data among the users, the application programs used to access data in the DBMS (StudyTonight, 2020).

iii. Data

Data is the most important component of the DBMS. The main purpose of DBMS is to process the data. In DBMS, databases are defined, constructed and then data is stored, updated and retrieved to and from the databases (StudyTonight, 2020). The database contains both the actual (or operational) data and the metadata (data about data or description about data).

iv. Procedures

Procedures refer to the instructions and rules that help to design the database and to use the DBMS (StudyTonight, 2020).

v. Database Access Language

The database access language is used to access the data to and from the database (StudyTonight, 2020). The users use the database access language to enter new data, change the existing data in database and to retrieve required data from database (Vaishnavi, 2020).

vi. Users

The users are the people who manage the databases and perform different operations on the databases in the database system (StudyTonight, 2020).

i. Application Programmers: This user group is involved in developing and designing the parts of DBMS.

ii. Database Administrator: A person responsible in managing the overall database management system.

iii. End-Users: These are the people who interact with the DBMS in performing different operations like inserting, deleting, updating and retrieving data etc.

The details of the voter and the admin are stored in the database for later use and the image taken is uploaded and stored into the database. The image taken and stored in the database during registration is then compared with the present face seen. This leads us to Facial Recognition which is used for image matching and for verification purposes.

2.2 FACIAL RECOGNITION

The word "biometrics" comes from the Greek terms "bio" (life) and "metrics," which mean "measurement" (to measure) (Mayhew, 2021). Given the significant rapid evolution of computer processing, efficient automated techniques have just gradually been viable. Many of these new automated procedures, on the other hand, are based on concepts that date back hundreds, if not thousands, of years.

Biometric identifiers cannot be tampered with or misplaced, and they represent any individual's identity, making them a key component of a personal identification system. Biometric recognition refers to the use of biometric identifiers such as the iris, fingerprint, face palm, and speech.

The face is one of the oldest and most fundamental instances of a trait that humans use to recognize each other. Faces have been used to identify known (familiar) and unknown (unfamiliar) individuals since the dawn of civilization (Mayhew, 2021).

Face recognition has become increasingly essential in recent years in extensive study. With the current global security scenario, governments and the commercial sector both demand dependable means to precisely identify persons without infringing on their privacy rights or requiring significant compliance on the part of the person being identified.

Biometric facial recognition, unlike other forms of identification such as passwords, email verification, selfies or photos, or fingerprint identification, employs unique mathematical and dynamic patterns that make it one of the safest and most successful.

The goal of face recognition is to discover a series of data of the same face in a database from an incoming image. The biggest challenge is ensuring that this process happens in real time, which is something that not all biometric face recognition software suppliers provide.

2.2.1 Facial Recognition Technologies

Several projects are competing for first place in the biometric innovation contest.

Google, Apple, Facebook, Amazon, and Microsoft (GAFAM) are all present and correct.

To advance our understanding as quickly as possible, all of the software online giants now disclose their theoretical breakthroughs in artificial intelligence, image analysis, and face analysis on a regular basis.

1. Academia

   Researchers at The Chinese University of Hong Kong developed the GaussianFace algorithm in 2014, which obtained face recognition scores of 98.52%, compared to 97.53% for people (Thales, 2021). It is a good rating despite flaws in memory capacity and calculation times.

2. Facebook

   Facebook revealed its DeepFace tool in 2014, which has a 97.25 percent accuracy rate in determining whether two photographed faces belong to the same individual. Humans answer properly in 97.53% of situations when taking the identical test, which is only 0.28% better than the Facebook computer (Thales, 2021).

3. Google:

   FaceNet, released in June 2015, took Google one step further. FaceNet set a new record for accuracy on the widely used Labeled Faces in the Wild (LFW) dataset, with a score of 99.63% (0.9963 ± 0.0009) (Thales, 2021). This technology is included into Google Photos and is used to automatically organize and classify photos depending on the persons identified. An artificial neural network and a novel technique to link a face to its owner with nearly flawless results.

4. Microsoft, IBM, and Megvii In February 2018, MIT researchers discovered that Microsoft, IBM, and China-based Megvii (FACE++) systems made more mistakes when detecting darker-skinned women than lighter-skinned men (Thales, 2021).

   In a blog post published at the end of June 2018, Microsoft revealed that its biased facial recognition algorithm had been significantly improved.

5. Amazon Rekognition is a cloud-based facial recognition program that was first made available to law enforcement organizations in May of 2018 (Thales, 2021). The software can identify up to 100 persons in a single image and perform face matches against databases with tens of millions of images.

Facial recognition system is used for authentication process, then this leads us to the blockchain which handles the voting process with transparency due to features of the blockchain.

2.3 BLOCKCHAIN

The blockchain concept is explained in this section. Haber and Stornetta first presented the blockchain concept in 1991. The major goal of creating an interfere timestamp for digital documents (Haber & Stornetta, 1991). Satoshi Nakamoto is thought to have created the first blockchain-based system in 2008. It's also worth noting that Bitcoin was the first major application of blockchain technology.

The term "blockchain" refers to a series of time-stamped and cryptographically connected blocks. The chain continues to expand as new blocks are added, with each new block retaining the hash of the previous block's information.

In summary, blockchain protects both private and public data against tampering and manipulation.

The goal of blockchain technology is to reinvent the concept of “trust” in a system by removing middlemen such as governments and businesses, which is the next generation architecture - decentralization. Instead of middlemen who are responsible for both data privacy and security, blockchain technology will place "confidence" in the system or "smart code".

2.3.1 Structure of Blockchain

Transactions in a blockchain network are validated by a community of nodes before being recorded in a block. A block is made up of a header and a body, the latter of which contains the transaction data (Figure 2.2). The previous block's hash, a timestamp, Nonce, and the Merkle root are all included in the block header (Figure 2.2). By submitting the header of the previous block to a hash function, the hash value is calculated. As a result of the former block's hash being kept in the current block, blockchain continues to develop as new blocks are created and connected to it. Furthermore, this ensures that tampering on the prior block will be noticed quickly.

The timestamp is used to keep track of when a block is produced. In the creation and verification of a block, once is utilized. The Merkle tree is a binary tree in which each leaf node is labelled with the hash of one transaction contained in the block body, and non-leaf nodes are labelled with the concatenation of its child nodes' hashes (Figure 2.2). Merkle root, or the Merkle tree's root hash, is used to shorten the time it takes to verify a block's transactions. Because a small change in one transaction can result in a drastically different Merkle root, the verification can be performed by only comparing the Merkle root rather than confirming all of the transactions in the block.

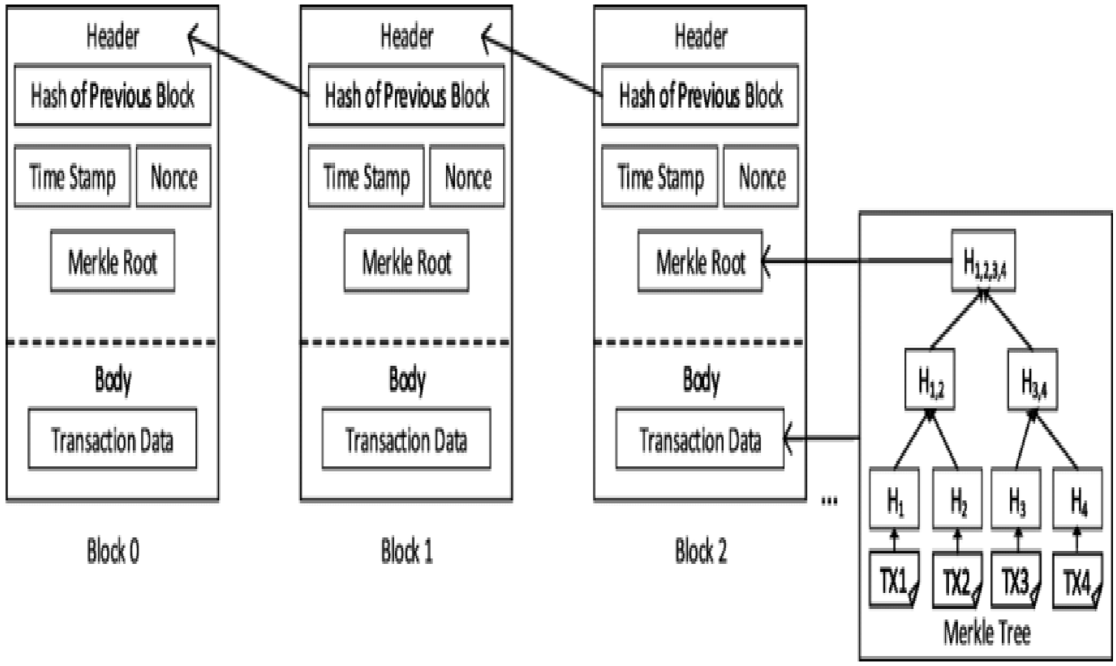


Figure 2.1 Blockchain Structure

Source: (Liang, 2020)

2.3.2 How Blockchain works

These are the core blockchain architecture components:

1. Node - This is a user or computer within the architecture and each one has an independent copy of the blockchain ledger.
2. Transaction - This is the reason of blockchain that serves as the smallest building block of a system such as records, information, etc.
3. Block - This is a data structure distributed to all the nodes in the network used for keeping transaction.
4. Chain - This is the sequence of blocks in an arranged manner.
5. Miners - These are specialized nodes that verify blocks before allowing anything to be added to the blockchain structure
6. Consensus (consensus protocol) - These are set of rules and procedures to carry out operations in blockchain.

A new transaction within the blockchain means the building of a new block. Each transaction is proven and digitally signed to prove its authenticity. The block is verified by the majority of the nodes in the system before it is added to the network.

A hash is like a fingerprint (long record that consists of some digits and letters). It is generated using cryptographic hash algorithm (SHA 256) and helps to identify a block in the structure easily. A block after being created is immediately attached to a hash.

Any attempts to corrupt the blocks will cause them to change. As a result, all subsequent blocks include inaccurate information, rendering the entire blockchain system invalid.

On the other hand, powerful computer processors may theoretically allow all of the blocks to be adjusted. However, there is a method known as proof-of-work that avoids this problem. All the nodes inside the architecture creates a consensus protocol and this is a set of network rules, and if followed by everyone, the rules becomes enforced inside the blockchain

2.3.3 Types of Blockchain

1. Public Blockchain

A Public Blockchain is a permission-less distributed ledger technology. It has no restrictions on who can access the network and make transactions as long as you have an internet connection access (DataFlair, 2018). The advantage of this type of blockchain is nobody will have complete control over the network. Therefore everyone will have equal authority making the blockchain fully distributed.

Examples are Bitcoin, Ethereum and Litecoin

2. Private Blockchain

A Private Blockchain is a permission or restrictive blockchain that operates in a closed network i.e. a restrictive network (DataFlair, 2018). These are usually used at a privately-held organization or company where only selected members are part of the network to store sensitive inforrmation. These networks are deployed for digital identity, asset ownership, voting, supply chain management, etc.

A network administrator is present in a private blockchain who handles user permissions in case a user requires extra authority on the go.

Examples are Multichain, Hyperledger projects (Fabric, Sawtooth), Corda, etc.

3. Consortium Blockchain

A consortium blockchain is a semi-decentralized type where more than one organization manages a blockchain network (DataFlair, 2018). It is a creative approach to solving organizations' needs where there is a need for public and private blockchain features.

Examples are Energy Web Foundation, R3, etc.

The types of blockchain with their properties differs and can be shown in table 2.1

Table 2.1: Comparison between the types of Blockchain

Source: (DataFlair, 2018)

Property	Public Blockchain	Private Blockchain	Consortium Blockchain
Consensus determination	All miners	Within one organization	Selected set of nodes
Read Permission	Public	Public or Restricted	Public or Restricted
Immutability level	Almost impossible to tamper	Could be tampered	Could be tampered
Efficiency (use of resources)	Low	High	High
Centralization	No	Yes	Partial
Consensus process	Permissionless	Needs Permission	Needs Permission

In blockchain, there is a computer protocol called smart contract which establishes the agreement between two parties written into lines of code.

2.4 SMART CONTRACTS

Simply said, a "smart contract" is a program that runs on Ethereum's blockchain. It's a set of commands (its functions) and data (its state) that lives on the Ethereum blockchain at a single address (Mehboob Khan et al., n.d.). They're often used to organize the executing of an agreement and deployed to the network so that all parties can be certain of the result right away, without the need for any middlemen or time wasting.

Simple “if/when...then...” statements are written into a code on the blockchain for smart contracts. When specified requirements are satisfied and validated, the activities are carried out by a network of computers. When a transaction is completed, the blockchain is updated. That means the transaction can't be modified, and the results are only visible to those who have been granted access.

There can be as many specifications as needed in a smart contract to convince the parties that the task will be executed correctly. Parties must identify how transactions and associated data are represented on the blockchain, examine any potential exceptions, and develop a framework for resolving disputes in order to set the terms.

After that, a developer can program the smart contract.

2.4.1 Application of Smart Contracts.

Smart contracts can be used across industries to automate business around the world.

1. Government: Smart contracts would solve difficulties by offering an infinitely more secure voting mechanism, as well as increasing citizen voting participation.
2. Supply Chain: Paper-based systems hinder supply networks by requiring approval from many channels, increasing the risk of fraud and loss. This is negated by blockchain,

which provides a secure digital version to chain participants and automates task and payment processing.

3. Real Estate: The ledger helps to save money because there is no need for middlemen. All you have to do is pay with bitcoin and have your contract encoded on the blockchain. Brokers, real estate brokers, hard money lenders, and anyone else involved in the real estate industry can profit.
4. Healthcare: Personal health records might be encoded and kept on the blockchain using a private key that only particular individuals would have access to. Surgical receipts might be maintained on a blockchain and forwarded to insurance companies as proof-of-delivery. The ledger could also be utilized for general healthcare administration, such as drug supervision, regulatory compliance, testing findings, and healthcare supply management.
5. Automobile: Smart contracts might operate as a "judge" to determine who was at fault in a crash: the sensor or the driver, among a slew of other factors. An automobile insurance business might charge variable premiums depending on where and under what conditions consumers drive their automobiles using smart contracts.

2.5 REVIEW OF EXISTING WORKS

In 2020, the paper titled Blockchain based E-voting System by Albin Benny (Benny, 2020) implemented an e-voting system as a smart contract for the Ethereum network using ethereum and solidity language. A biometric device was used for validation service during registration. The project explored the potential of using decentralized networks enabling more auditing and understanding of elections.

In 2018, the paper titled Blockchain based E-Voting system by Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson (Hjalmarsson et al., 2018) aimed to evaluate the application of blockchain as service to implement distributed electronic voting systems. It identified the legal and technological limitations of using blockchain as a service for systems. The proposed system was a blockchain-based system using permissioned blockchain and smart contracts to advance from a pen and paper scheme to a time-efficient and cost scheme while increasing the security to enable liquid democracy.

In 2018, the paper titled A Study on Decentralized E-Voting System Using Blockchain Technology by Mrs. Harsha V. Patil, Mrs. Kanchan G. Rathi, Mrs. Malati V. Tribhuwan (Patil et al., 2018) used a decentralized blockchain system with encryption to promote participation, address vote tampering, promote great transparency to voters and made individual votes publicly while protecting voters. However, the drawbacks are the technology faced resistance from the political leaders who befitted from the status and the complexity of the system.

In 2020, the paper titled Decentralized Electronic Voting System Based on Blockchain Technology Developing Principals by Kateryna Isirova, Anastasiia Kiian, Mariia Rodinko and Alexandr Kuznetsov (Isirova et al., 2020) proposed a decentralized electronic voting system using blockchain. The two-level architecture provides a safe process without redundancy of existing systems. The proposed system has six steps to ensure requirements are put forward for voting transparency and anonymity. There is no central trust point absence, as a result there is no directed attack aim.

In 2019, the paper titled Securing Voting System using Blockchain and Fingerprint Verification by Miss. Komal Kundan Sharma, Prof. Mrunalinee Patole, and Prof. Vina M. Lomte (Sharma et al., 2019) proposed a permission based multichain platform for voting, Multichain is a new software development that allows the arrangement of your own Blockchain approach. Fingerprint recognition is used for voter's identity authentication and is useful towards a secure voting system.

In 2018, the paper titled Crypto-Voting, a blockchain based e-voting system by Francesco Fusco1, Maria Ilaria Lunesu, Filippo Eros Pani and Andrea Pinna (Fusco et al., 2018) implemented a system called Crypto-voting based on permissioneed blockchain technology using two linked blockchains, one-way pegged sidechain. The first sidechain records voters and the voting procedures, the second sidechain calculates the votes and produces the results. This system increased the efficiency of validation phase and assignment of the candidate's vote. It also encouraged voting from remote locations and removal of middlemen.

In 2017, the paper titled Blockchain based e-voting recording system design by Rifa Hanifatunnisa and Budi Rahardjo (Hanifatunnisa & Rahardjo, 2018) proposed a method using SHA256 hash functions that works as a fingerprint of a data and seeked for any harms possible on SHA-256. It strongly recommended to use SHA256 with its algorithm that has proven safe used with cryptographic algorithms.

In 2020, the paper titled Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for National Elections by Olawande Daramola and Darren Thebus (Daramola & Thebus, 2020) demonstrated how the architecture trade-off analysis method (ATAM) could be used to enable election stakeholders to understand potential risks, challenges and prospects of blockchain e-voting through a participatory architecture assessment and documentation process. A security analysis was enabled by the Hyperledger

Fabric (HF) that can protect the Blockchain-based architecture for national e-voting system from security threats during a national election.

In 2019, the paper titled Blockchain Based Secured E-voting by using the Assistance of Smart Contract by Kazi Sadia, Md Masuduzzaman, Rajib Kumar Paul and Anik Islam Abhi (Sadia et al., 2019) proposed a system that uses smart contract that deals with security issues, accuracy and voters' privacy during the vote. This results in a transparent, non-editable and independently verifiable procedures that discards fraudulent activities. There is reduction of third party completely that shows proof of healthy election.

In 2020, the paper titled Blockchain-based Electronic Voting System with Special Ballot and Block Structures that Complies with Indonesian Principle of Voting by Gottfried C. Prasetyadi, Achmad Benny Mutiara and Rina Refianti (Prasetyadi et al., 2020) proposed a ballot designed as block transaction employing UUID version 4, a modified block structure using SHA3-256 hash algorithm and a voting algorithm. The received ballots could be checked for authenticity and integrity using Elliptic Digital Signature Algorithm (ECDSA), and then all data in each ballot were checked for validity. Only valid ballots could be recorded as transaction, which were then mined into blocks and if a node had one or more tampered transactions, they could be detected and restored by comparing the data with other node.

In 2018, the paper titled Secure Digital Voting System based on Blockchain Technology by Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan (Khan et al., 2018) presented an effort to leverage benefits of blockchain such as cryptographic foundations and transparency to achieve an effective scheme for e-voting. It is implemented with Multichain and in-depth evaluation of approach highlights its effectiveness to achieve an end-to-end e-voting scheme.

In 2019, the paper titled Election System Based on Blockchain Technology by Noor Mohammedali and Ali Al-Sherbaz (Mohammedali & Al-Sherbaz, 2019) proposes a decision-making framework based on innovation to create a secure, unjustifiable, accurate and transparent framework for voter privacy. Also each square in the blockchain innovation that relates to the previous square contains the hash of the previous square, and each square contains explicit data based on the square footage. The hub is connected by a peer network in this framework, with all the hubs in the block site network that have a complete duplicate block. The SHA512 extension algorithm is used to redeem the block information and Elliptic Digital Signature Algorithm (ECDSA) digital signature algorithm is used to verify and validate the character.

In 2020, the paper titled Blockchain Based Secure Voting System Using IoT by Dr.R.Suganya1, A.Sureshkumar, P.Alaguvathana, Ms.S.Priyadharshini, K. Jeevanantham (Suganya et al., 2020) proposed a system using blockchain and hashing method to provide the anonymity of the voter. The distributed system in blockchain technology provides transparency and the centralized system can be replaced by distributed ledger technology which prevents attacker from modifying the result. A fingerprint module is going to be merged to the voting matching to verify the ID.

In 2018, the paper titled Blockchain-Based Electronic Voting Protocol by Clement Chan Zheng Wei, Chai Wen Chuah (Wei & Wen, 2018) proposed a blockchain-based electronic voting protocol in this paper. The electronic voting system makes use of blockchain technology properties to enhance its security features. The system can secure the identity of every voter and ensure that all the vote results recorded are tamper-proof. Blockchain provides advantageous properties for e-voting system such as authenticity, integrity, verifiability, anonymity, availability and a general consensus from every participant. The system does not rely on human trust but on computational cryptographic trust. This blockchain-based electronic voting protocol is secure in a way that no one is able to corrupt it.

In 2019, the paper titled securing e-voting based on blockchain P2P network by Haibo Yi (Yi, 2019) presented techniques to exploit blockchain in P2P network to improve the security of e-voting. A synchronized model of voting records based on distributed ledger technology (DLT) to avoid forged votes is designed then, a user credential model based on elliptic curve cryptography (ECC) to provide authentication is designed and lastly, a withdrawal model is designed to allow voters change their votes before a preset deadline. All votes in the blockchain is cryptographically linked block by block.

CHAPTER 3

METHODOLOGY

3.1 SYSTEM ANALYSIS

This is a method of recognizing issues, acquiring, organizing, and analyzing information about the issue. The study of a system or its components in order to determine its goals is known as system analysis. This method is used to fix problems by improving the system and ensuring that all of the system's components work together effectively to achieve the system's goal. It defines what a system should be capable of.

3.1.1 Analysis of existing system

The existing system involves the process of using Public Permissionless Blockchain and smart contracts. Anyone can access the Blockchain with a laptop/mobile device and internet. Voters registers and log-in to vote. After voting, the voter still has the permission to change their vote within the election duration. The voter can view the result after it’s been casted.

3.1.2 Drawbacks of Existing System

The drawback of the existing system is that of security because there is no way to differentiate peoples face and could lead to impersonation of another person.

3.2 ANALYSIS OF NEW SYSTEM

The proposed voting system will allow voters to vote using a mobile device from any location. Each voter would be enrolled into the database through the collection of their names, sex, date of birth, state, LGA, phone number, ethereum private key and face ID. When it is time for election, the voter logs in to the system with their email address and password, verifies face with the facial recognition system and proceeds to vote. The vote is counted and the results can be reviewed.

3.2.1 Benefits of New System

1. It will give the Electoral Commission a way to organize elections that are less expensive and more fair, as well as cut down on the time spent collating and releasing results.
2. Backup: Documents are safeguarded because they are duplicated and shared over the network ensuring credible elections.
3. Trust: It increases citizens' participation in the election process due to its transparency and the votes are encrypted in a shared ledger.
4. It allows people to vote from the comfort of their own homes because it integrates remote voting.
5. It is a decentralized system, there is no need of a third party (middlemen) incase of manipulation of results.
6. The security level is high and not prone to cyberattacks.

3.3 REQUIREMENTS ANALYSIS AND SPECIFICATION

The requirements for an e-voting system to be developed to model the Nigerian election at the Federal level and provide a solution to voters' apathy are listed below;

1. The system should allow voters to register and vote for their place of origin from any place of residence or convenience.
2. The system should scan and store voters' faces for authentication purpose.
3. The system software platform should be accessible to eligible voters.
4. The system should process biometric data with speed
5. The voter should be able to use the interface easily.

6. The database should have integrity data.
7. The voter should not experience lagging when using the system.

3.4 SYSTEM DESIGN

3.4.1 Architectural Design

The architecture of a system depicts how various components interact to achieve the main goal (Figure 3.1). The Administrator logs in, initiates, set up the election and publish result. The voter registers into the system with their names, date of birth, etc. The voters' data are collected including their faceprint and stored in the database. On the Election Day, the voters logs in to the system using their email and password and are taken to the facial recognition screen. The system scans the face and automatically checks if the face matches the image stored for the voter in the database. If it is a match, the voter proceeds to cast a vote by selecting their candidate and clicking the button. The voter can also view the results as the election is going on. The Administrator announces the vote results (seen in figure 3.1).

3.4.2 The working principle

In fact, for successful facial recognition, the technology takes into account the face geometry (including the length of the jawline, the form of the cheekbones, the depth of the eye sockets, and so on). All of these elements aid the technology in "remembering" who owns the face. The camera recognizes and tracks the image of a face. A picture of the face is taken and examined. Most facial recognition technology uses 2D images rather than 3D images because it is easier to match a 2D image with those in a database. The face's geometry is read by the software. Based on a person's facial traits, the face capture method converts analog information (a face) into a set of digital information (data). The examination of the voters face is effectively reduced to a mathematical formula. Faceprint refers to the numerical code. Each voter has their own faceprint, similar to how thumbprints are unique. After then, the faceprint is compared to the database of other people's faces (Figure 3.2). A determination is made if your faceprint matches an image in a facial recognition database.

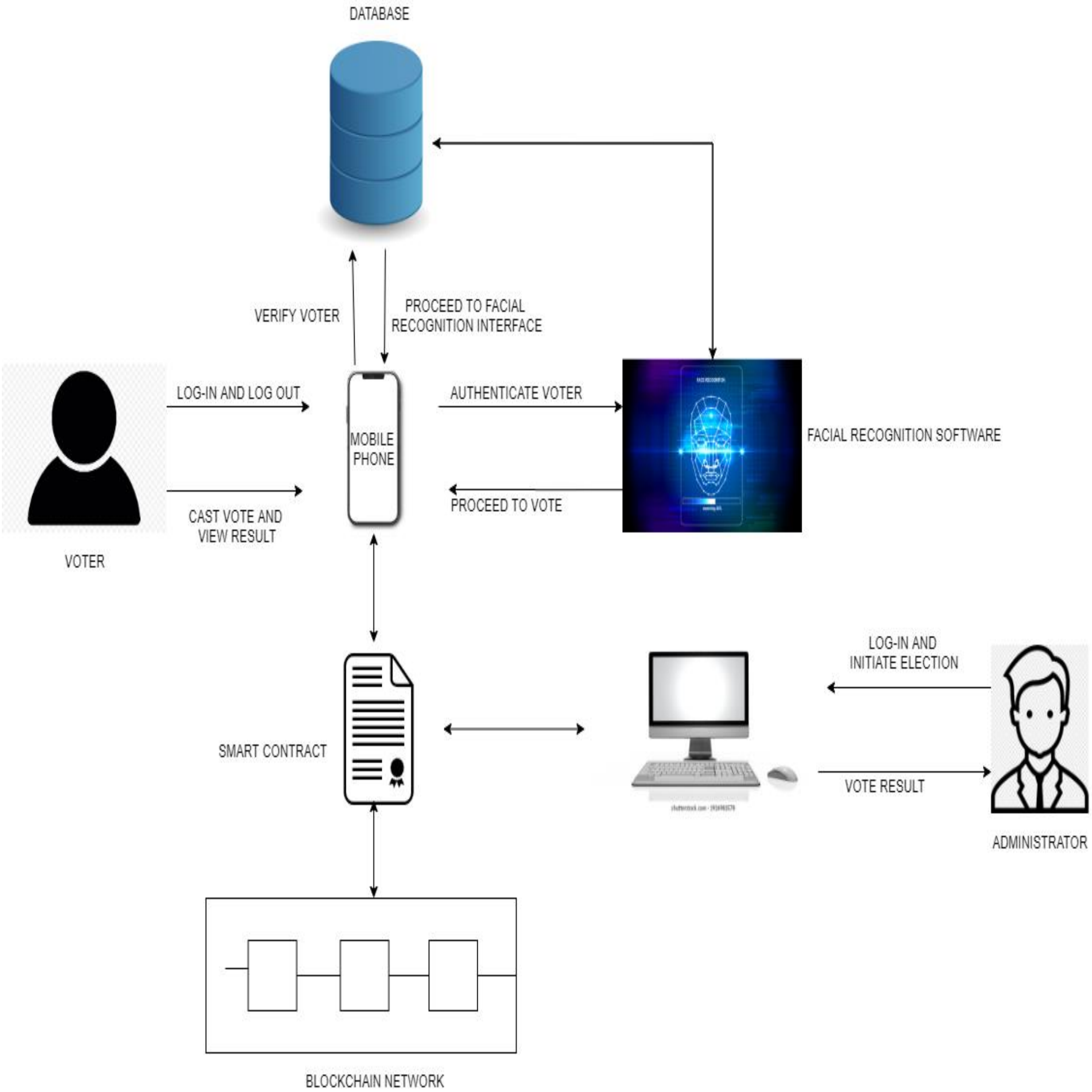


Figure 3.1: Architecture of the system

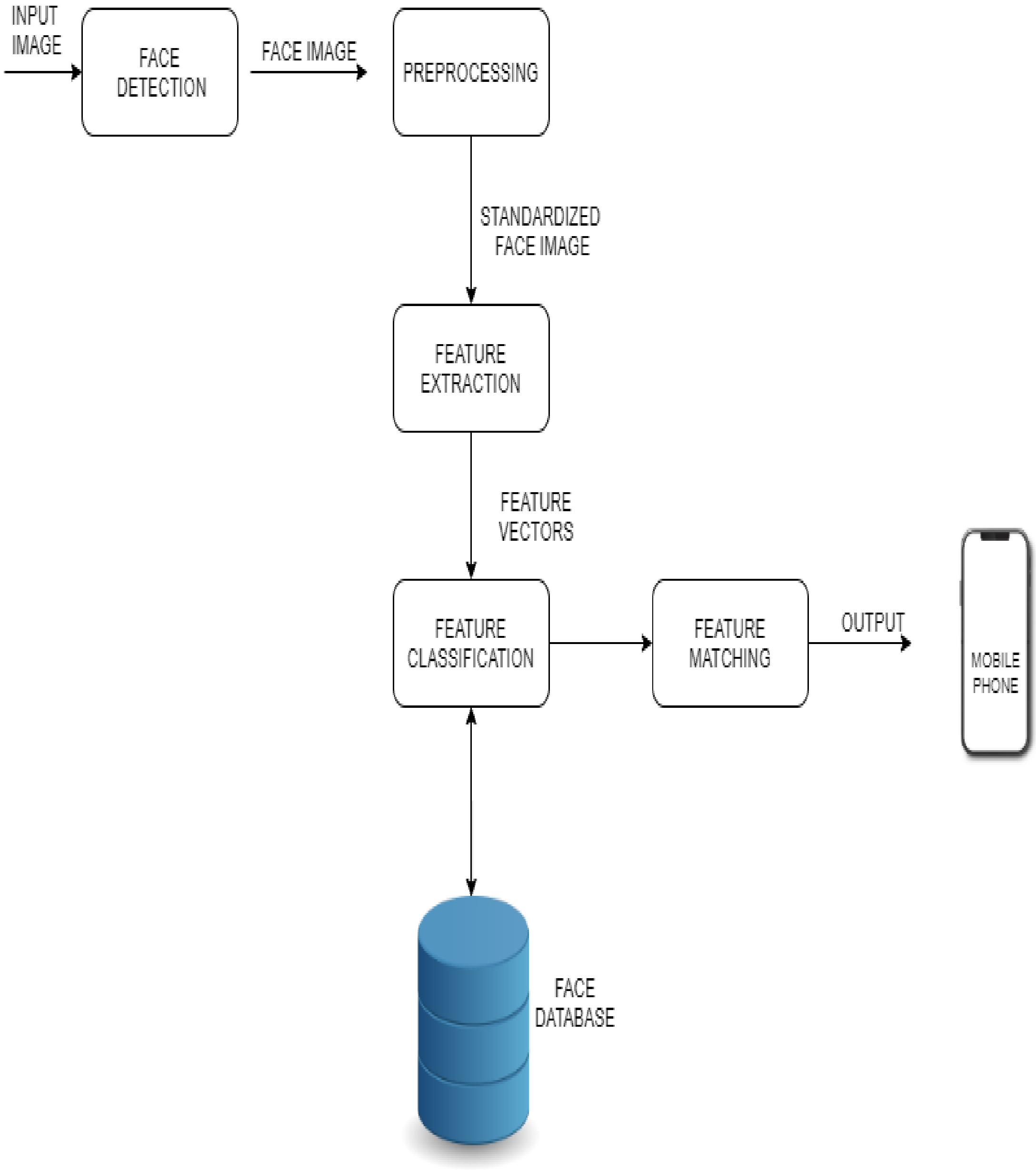


Figure 3.2: Block Diagram of a Face Recognition System

3.4.3 Use case diagram of the System

The use case diagram is a visual representation of how a user interacts with the technology under discussion. It depicts all possible interactions or activities between the actors (Voters and Administrator) in the system (Figure 3.3).

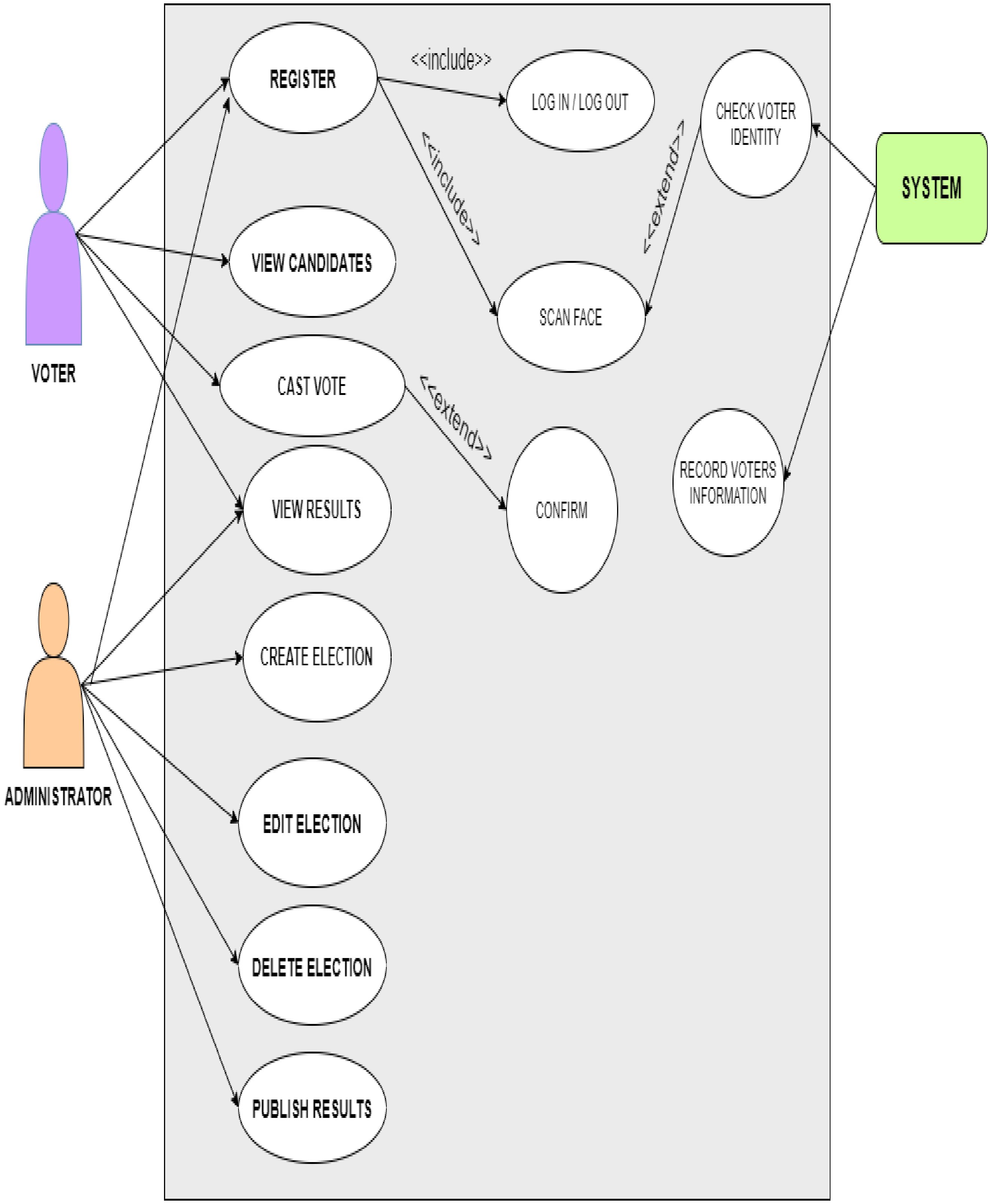


Figure 3.3: Use Case diagram of the system

3.4.4 Flowchart of the System

The system's flowchart depicts the steps involved in its implementation.

The voting page is the software that runs on an electronic device that allows voters to cast their vote (Figure 3.4).

The registration page is where the voters are registered prior to the election. It involves collecting voters' data and storing data in the database through the server (Figure 3.5).

The Registration page requires the following voter details listed below

1. Voters names
2. Gender
3. Date of Birth
4. State
5. Local Government Area (L.G.A)
6. Phone number
7. Email
8. Face ID

The administrator dashboard is a software application managing the election. It includes functionality for monitoring voters, create elections and to view results. To prevent unauthorized access to the administrator dashboard, there is a login page, as seen below. For authentication, the login will require the administrator's email address and password, which will be validated against database values. If validation is successful, the admin is validated using a facial recognition interface and provided valid dashboard access. Below is a flowchart (Figure 3.6) for the admin dashboard function.

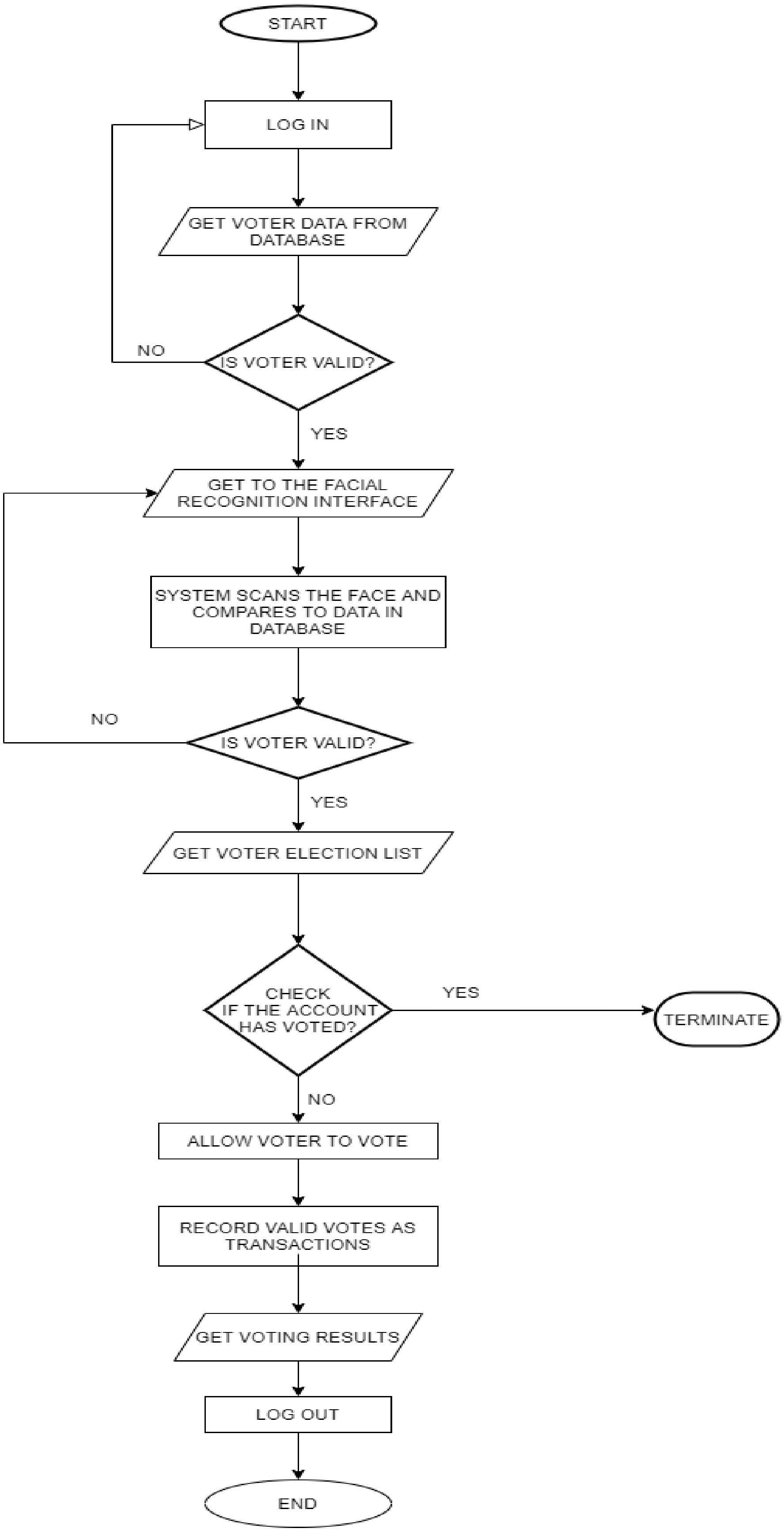


Figure 3.4: Voting Page

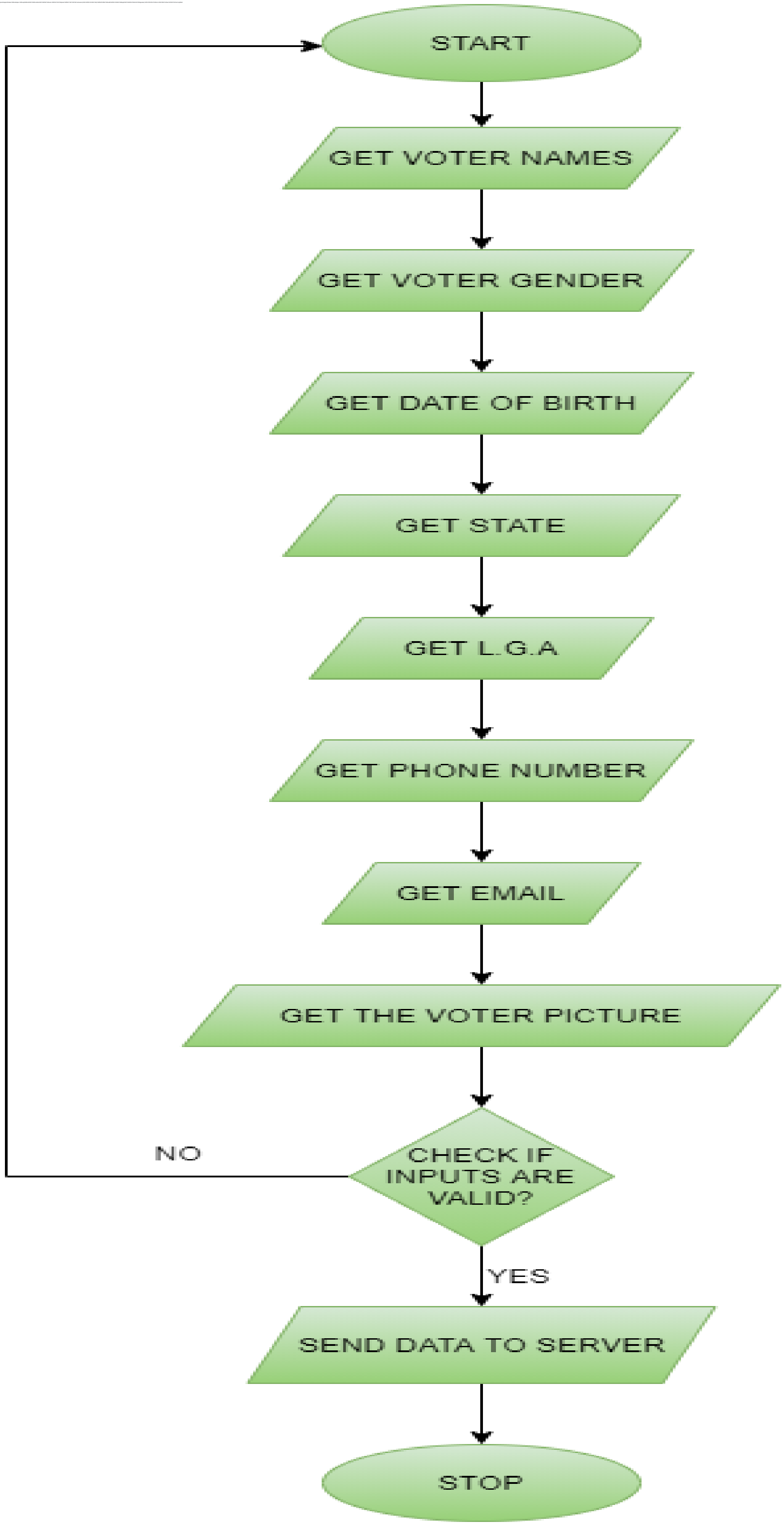


Figure 3.5: Registration Page

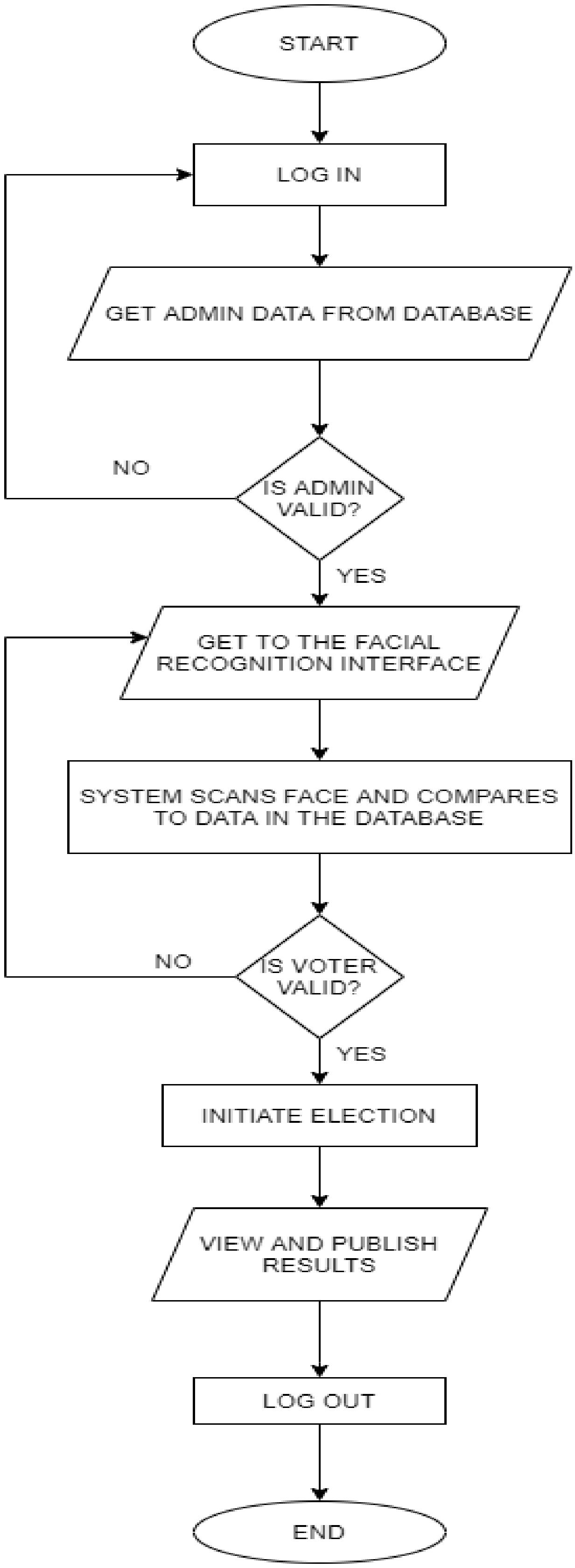


Figure 3.6 Administrator Dashoard

3.5 SYSTEM DEVELOPMENT

A mobile application would be developed for the system.

The mobile application would be develop using Flutter. The blockchain would be integrated into the app so the user can vote and view the results.

The tools to be used for the development includes:

i. Flutter

Flutter is an open-source UI software development kit (SDK) created by Google. It is used to develop cross platform applications for Android, iOS, Linux, Mac, Windows, Google Fuchsia, and the web from a single codebase.

ii. Visual Studio Code

Microsoft's Visual Studio Code is a cross-platform integrated development environment (IDE) for Windows, Linux, and macOS. Debugging, syntax highlighting, intelligent code completion, snippets, code refactoring, and embedded Git are among the features.

iii. Solidity

Solidity is an object-oriented programming (OOP) language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum.

iv. Ganache

Ganache is a personal blockchain for rapid Ethereum and Corda distributed application development. It is used for testing Solidity contracts

v. PresentID

PresentID is a facial recognition software where images are submitted into the API, and the faces found are analyzed, then the API returns a bunch of useful data about the faces found. This is used to combat online fraud and authetication using combination of Voice, Face and ID Card OCR.

3.6 SYSTEM TESTING

This would be tested by the voters whose feedback would be used to evaluate the system.

CHAPTER 4

SYSTEM IMPLEMENTATION AND RESULTS

This chapter provides a detailed description of the system's implementation, including the implementation of the e-voting system. This phase of system development includes the hardware and software requirements, implementation and testing of the developed software. The implementation refers to all of the activities that were carried out and put in place in order to put the developed system into operation using the methodology's approach (i.e. architectural diagram, use case diagram, and flowchart) in order to achieve the project's objectives and convert the theoretical design into a working system. The components of the system were also tested and evaluated.

4.1 INSTALLATION REQUIREMENTS

4.1.1 Hardware Requirements

The hardware are physical components of a computer system that are can be seen and touched. The hardware requirement of the system includes:

i. A laptop or desktop computer (Preferably 64bit)
ii. Random Access Memory (RAM): 8 GB Minimum
iii. Processor: Intel Core i5, 2.4 GHz Minimum

4.1.2 Software Requirements

The software includes both the system and application software installed for the development of the system. The software requirements of this system include:

i. Windows Operating System (8/10)
ii. Visual Studio Code
iii. Webstorm

iv. Flutter

v. Genache

4.2 GENERAL WORKING OF THE SYSTEM

The electronic voting system was deployed on a mobile application. It was developed to encourage remote voting and make the system user friendly.

The Blockchain based electronic facial recognition voting software has the following pages:

4.2.1 The Split screen Page

The splash screen introduces the application to the user and an option to proceed to the log-in page (Figure 4.1). The splash screen automatically changes after one second to the get started screen. The get started screen has two options (Figure 4.2), to create a voter account or Log-in as admin.

The goal of the split screen page is to visually communicate value to the application so that it is both branded and user friendly.

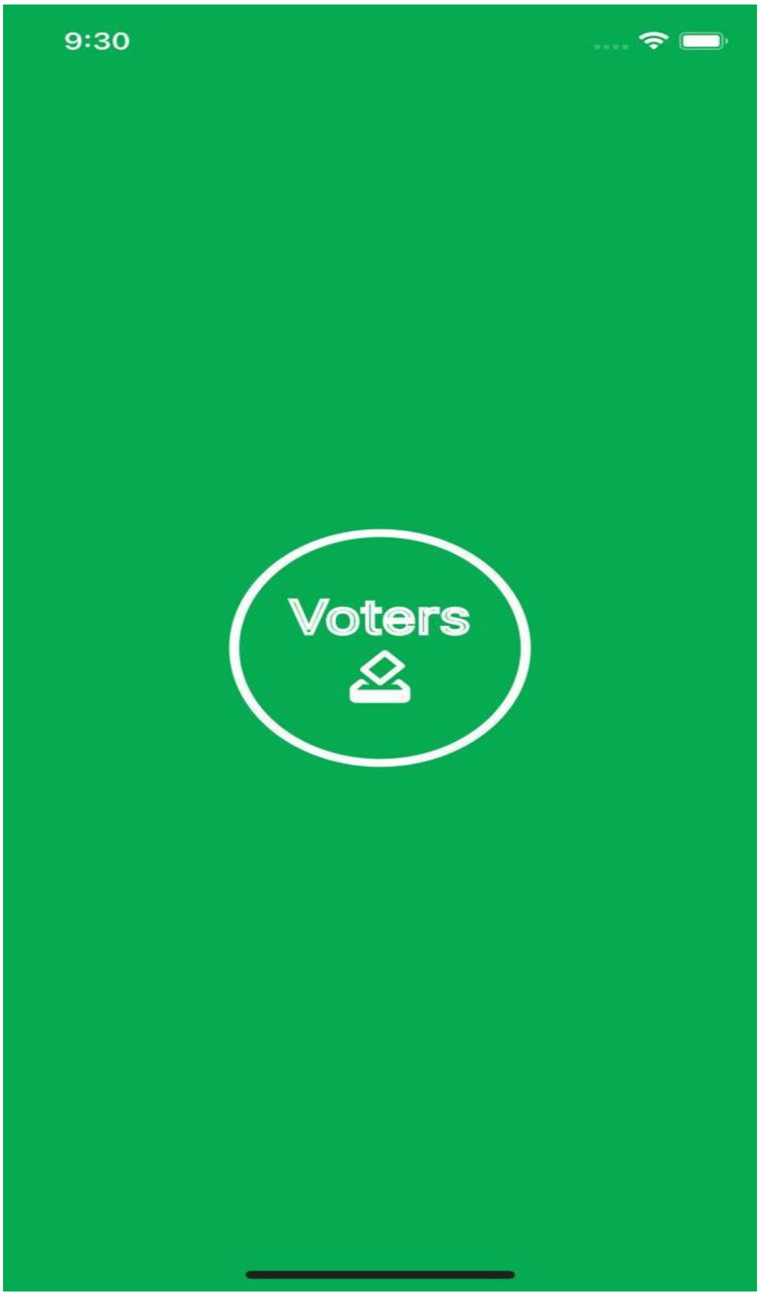


Figure 4.1: Splash Screen Page

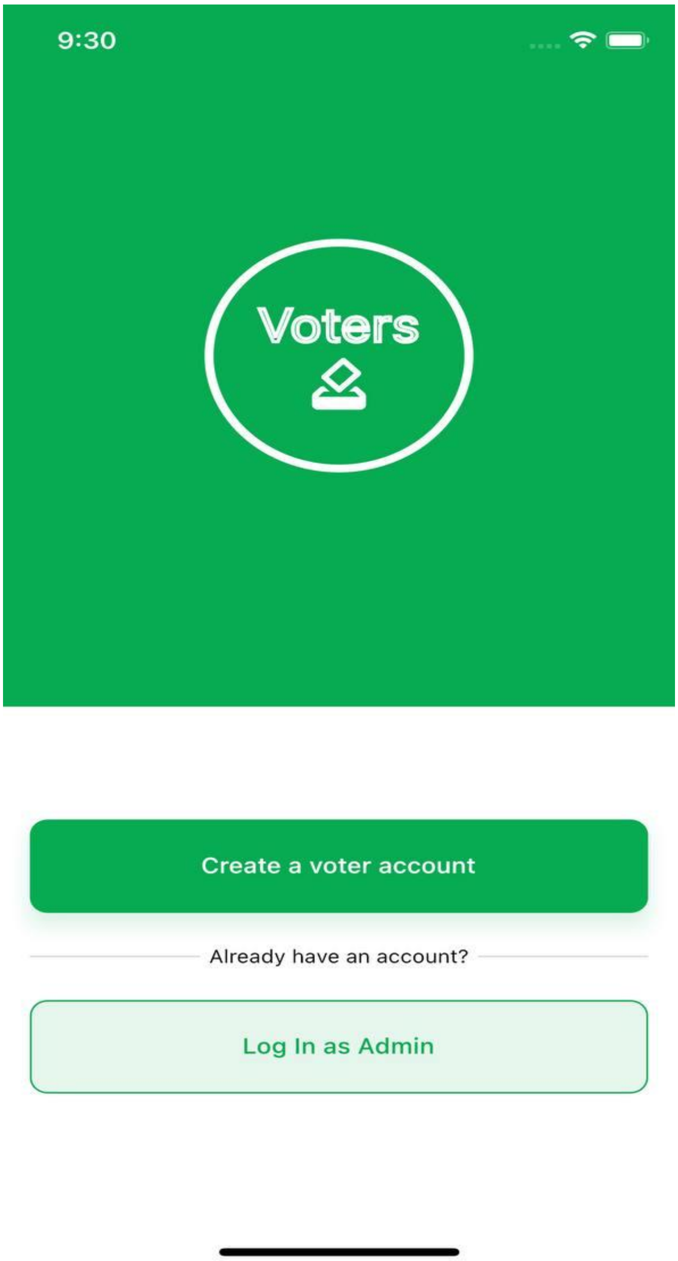


Figure 4.2: Get Started Screen Page

4.2.2 The Login Page

The Voter Login page consists of a form that asks registered voters to fill in their private key. New voters are required to click on the Create a Voter Account which takes them to the Register page (See figure 4.3).

The Admin Log-in page consists of a form requiring the email address and password of the admin (Figure 4.4).

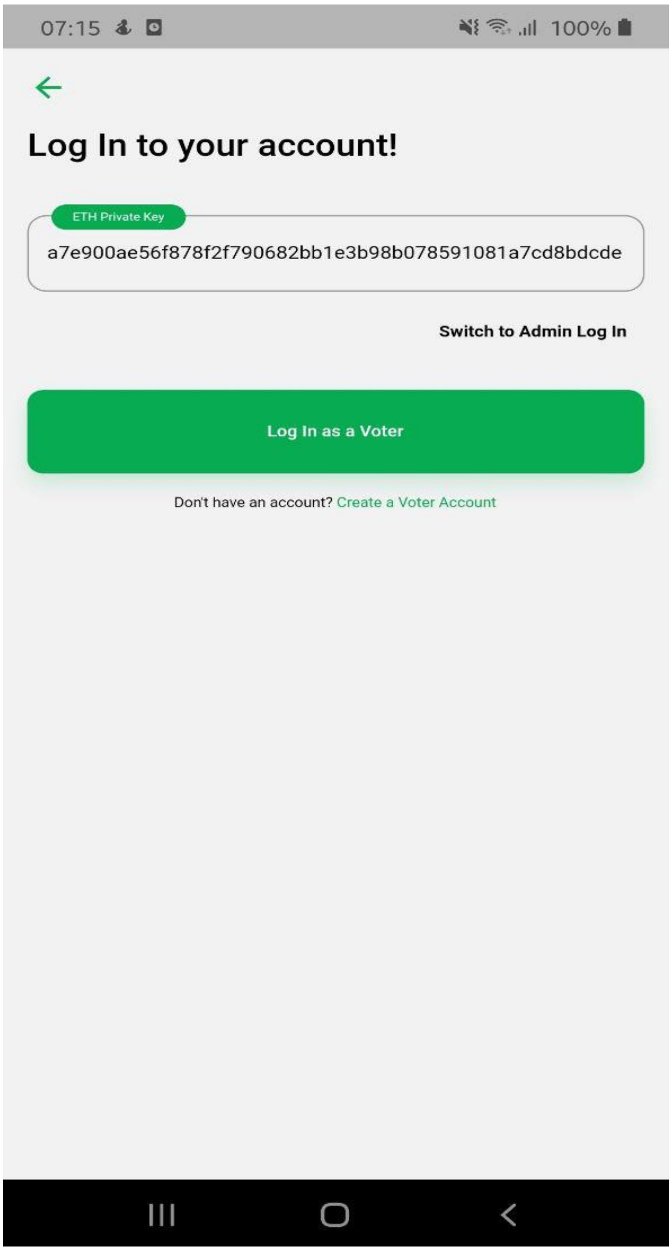


Figure 4.3: Voters Login page

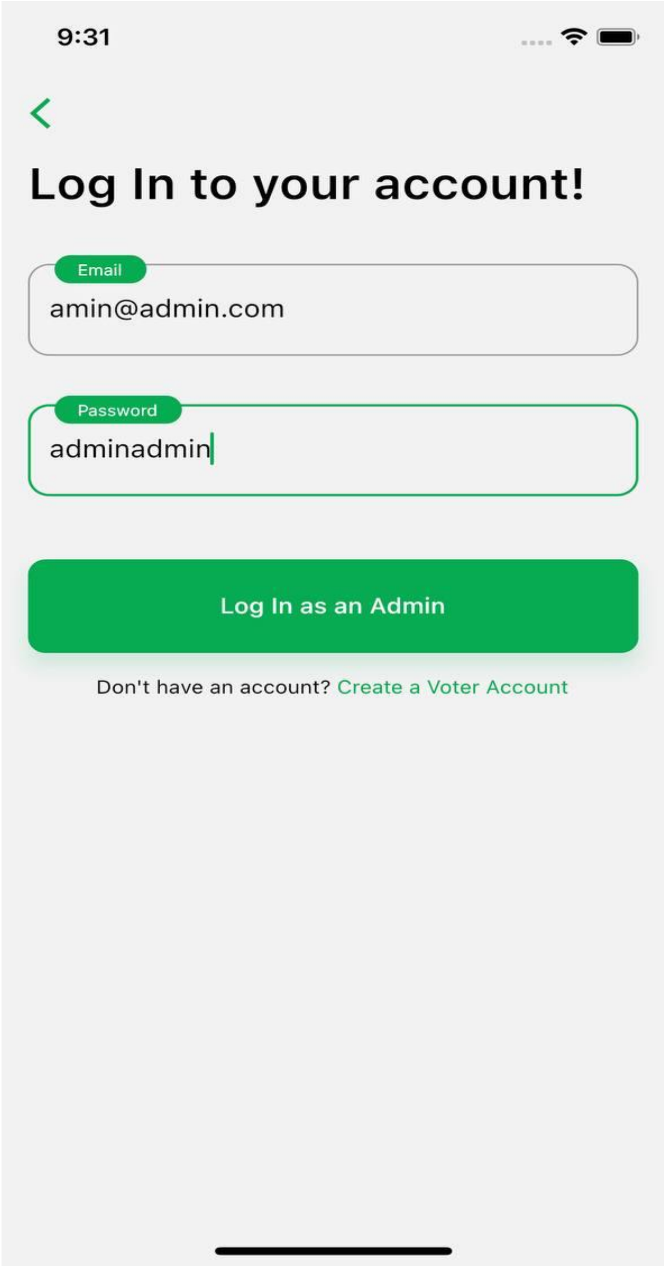


Figure 4.4: Admin Login Page

4.2.3 The Registration page

The voter provides information about themselves. This information includes private key, first name, last name, email address, and phone number, date of birth, state, gender, LGA and password (Figure 4.5). The purpose of this page is to gather information about the voter.

4.2.4 Voter Dashboard page

The voter dashboard page is divided into 2 sections. The first section is the profile page which contains information about the voter (Figure 4.6). A “Logout” button is used to sign out a voter’s details from the system and redirects them to the Log-In page.

The second section is the election page which contains information about the upcoming elections, the positions, the candidates running for a position and the results (Figure 4.7).

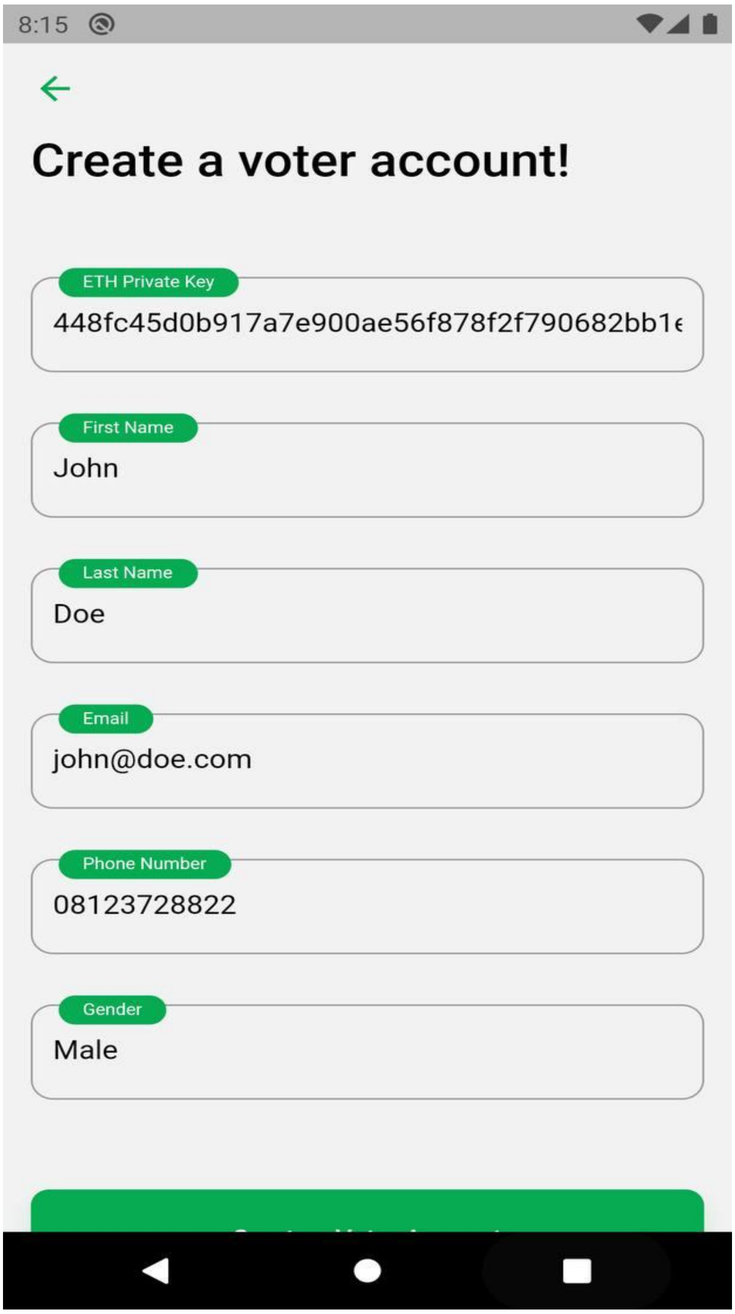


Figure 4.5: Registration page

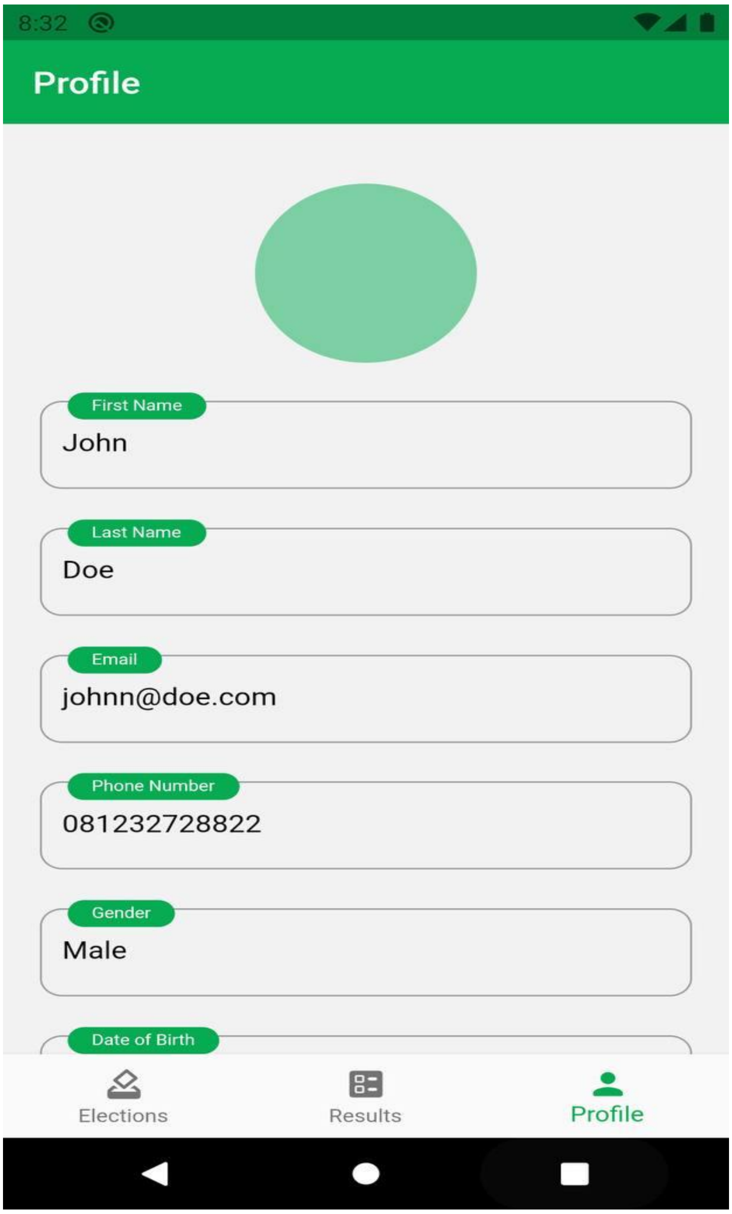


Figure 4.6: Voters Profile Page

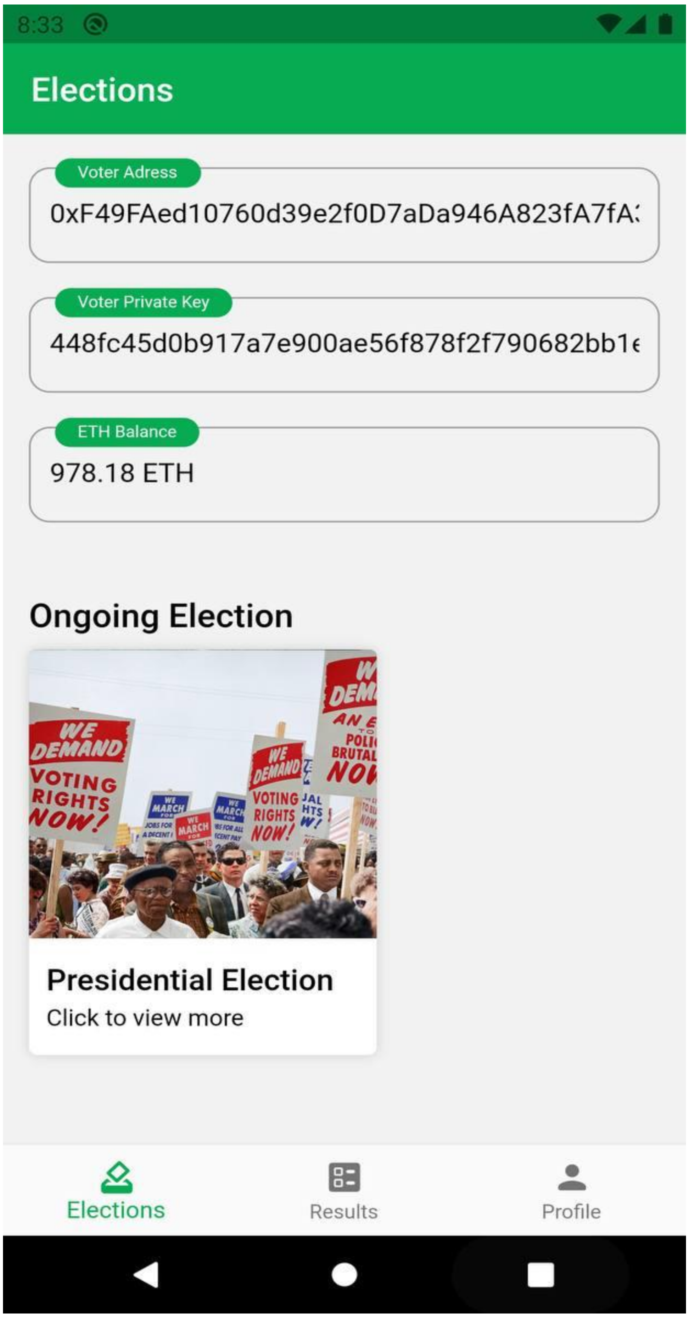


Figure 4.7: Voter Election Page

4.2.5 The Voting Page

The voters has the right to choose their desired candidate for the position. The page contains information about the candidates and a “vote” button to make their choice (Figure 4.8).

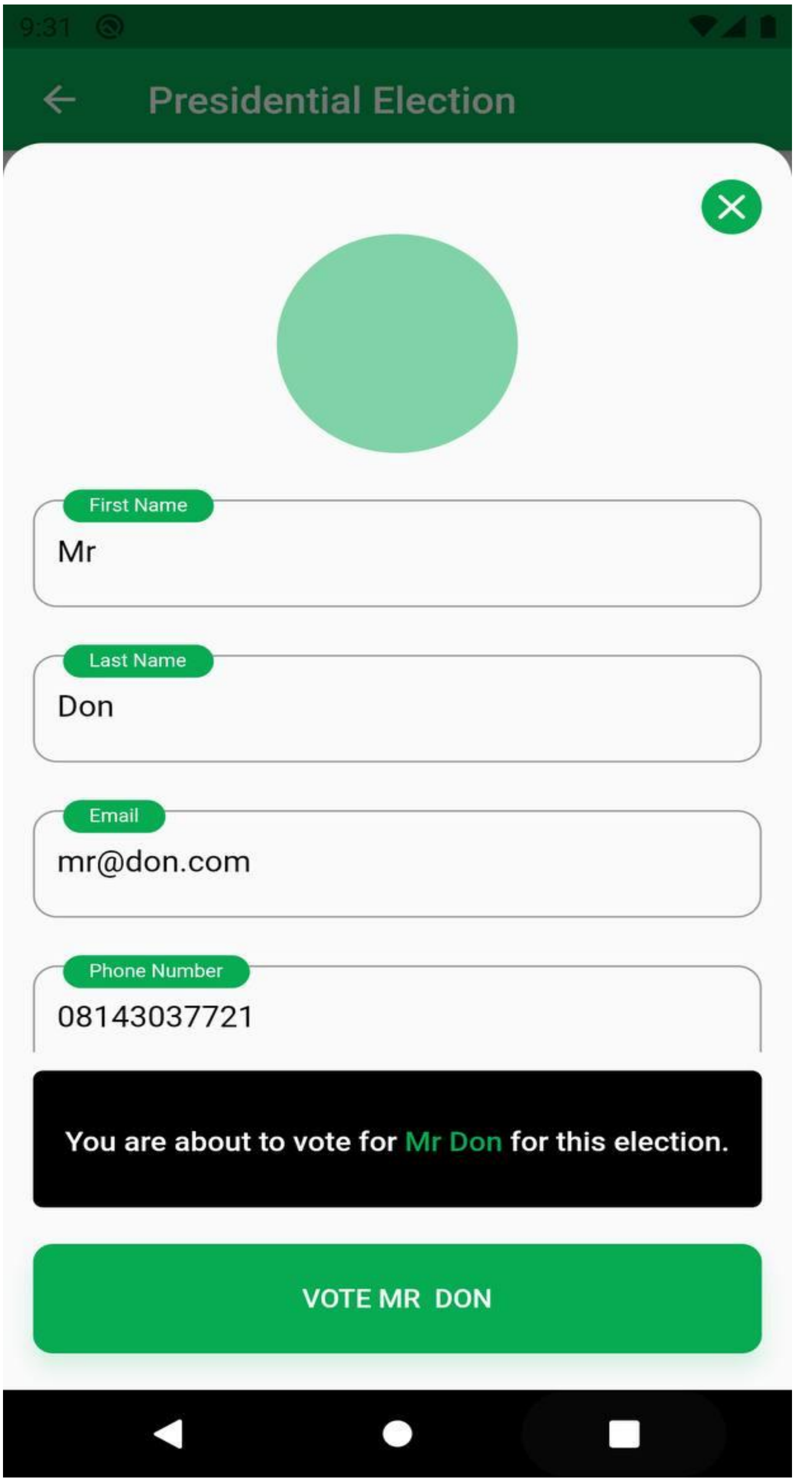


Figure 4.8: Voters vote page

4.2.6 Administrator Dashboard Page

The administrator dashboard page is divided into 4 sections; the election screen, voters screen, results screen, profile screen. The first section is the profile page which contains information about the admin (Figure 4.9). A “Logout” button is used to sign out the admin’s details from the system and redirects to the Log-In page.

The second section is the election page which contains information about the upcoming elections, the positions, the candidates running for a position and the results (Figure 4.7).

The third section is the voters’ page. The purpose of this page is for the admin to supervise all the voters and check if they have voted (Figure 4.11).

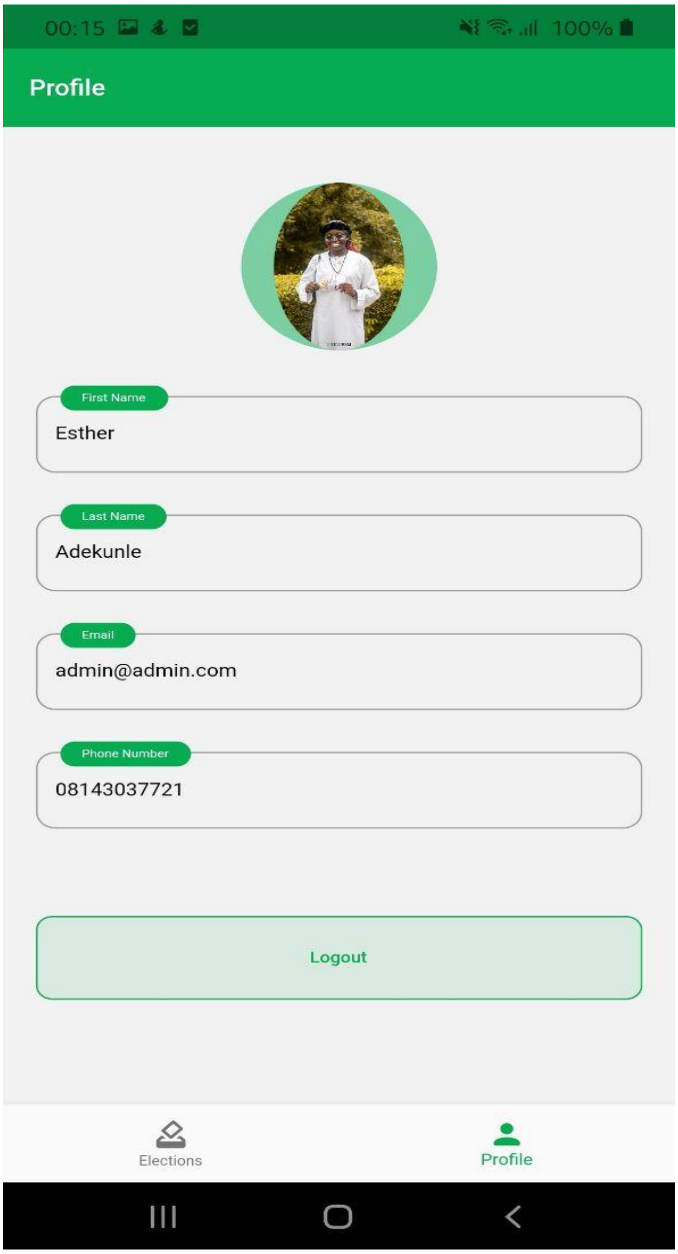


Figure 4.9: Admin profile page

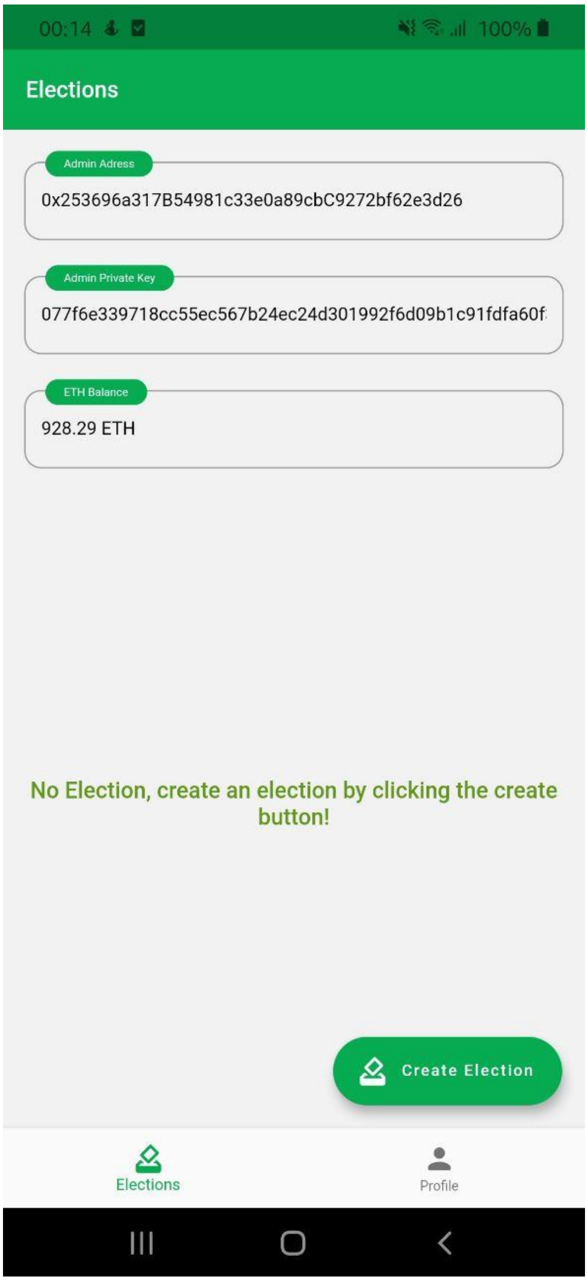


Figure 4.10: Election Page

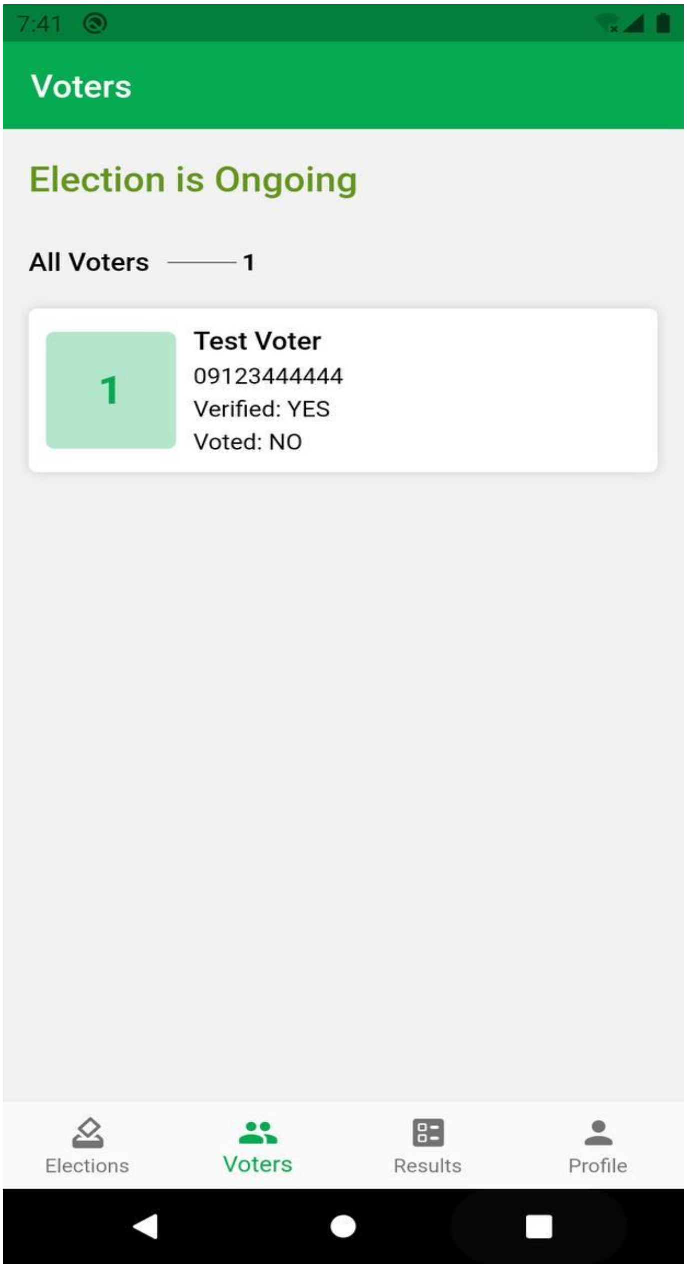


Figure 4.11: Admin voters' page

4.2.7 Create Election Page

The admin creates the election. It is divided into three; the first step is to create the election setting the election name, election description and the voting date (Figure 4.12).

The second step is to create position based on the election by setting the position name and their descriptions (Figure 4.13).

The third step is to create candidate based on the position by setting the name, phone number, date of birth, state, LGA, image and gender. See Figure 4.14

The Admin election screen shows added candidates. See Figure 4.15

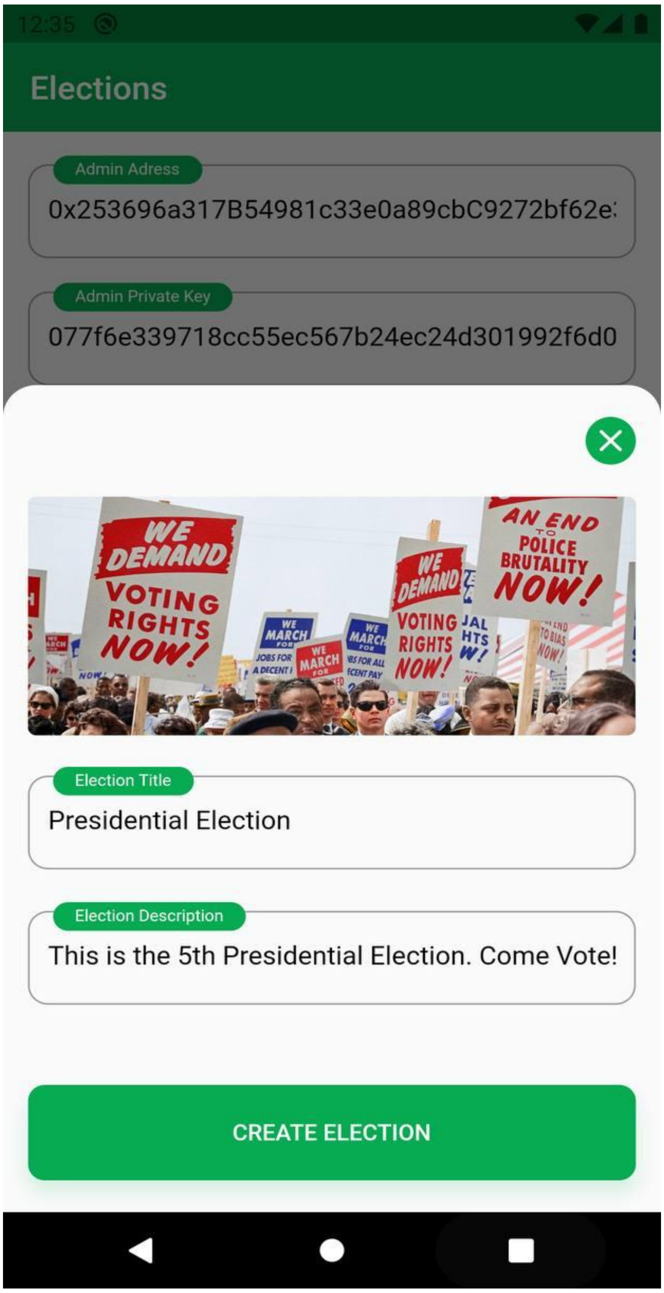


Figure 4.12: Create Election pop up page

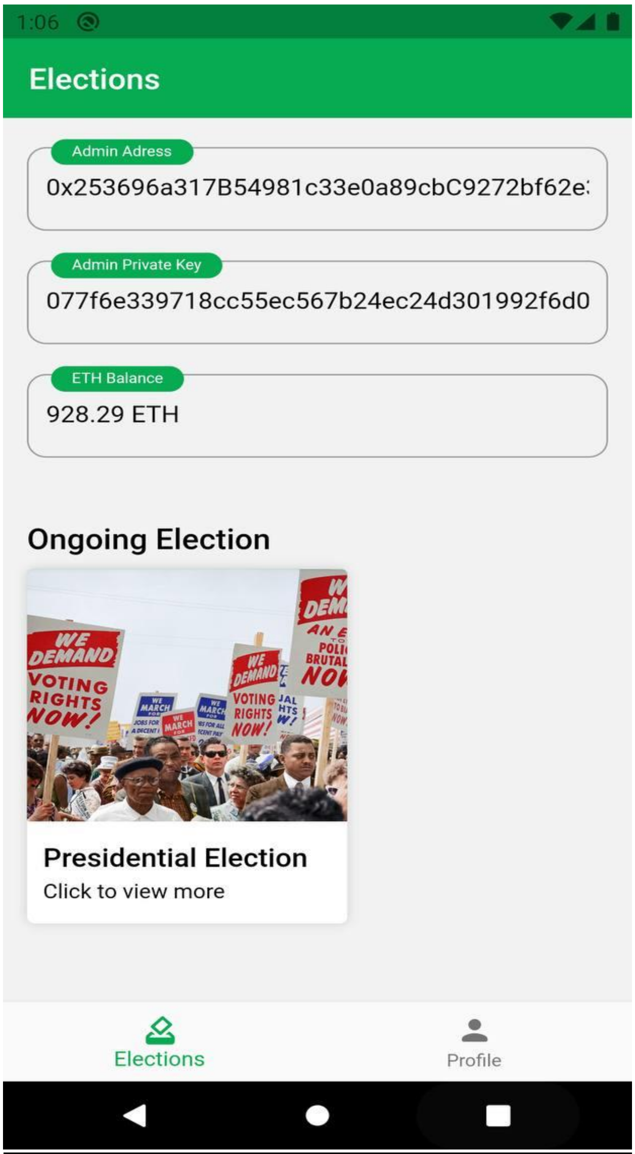


Figure 4.13: Ongoing Election page

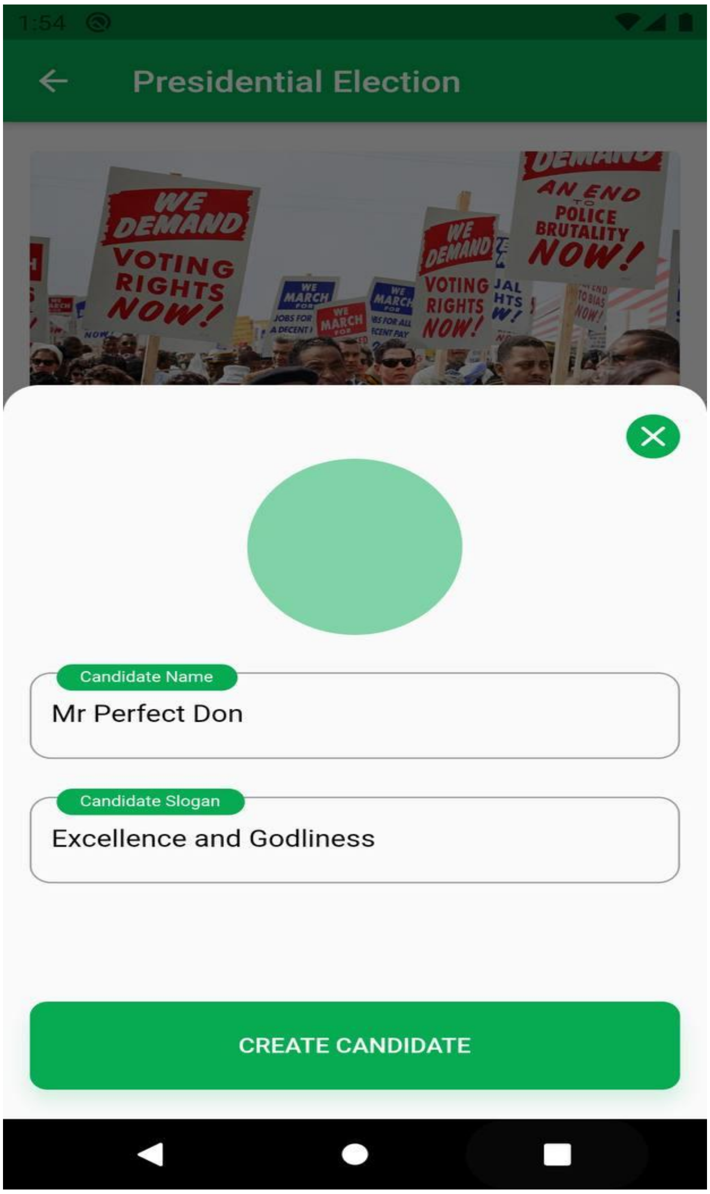


Figure 4.13: Create Candidate page

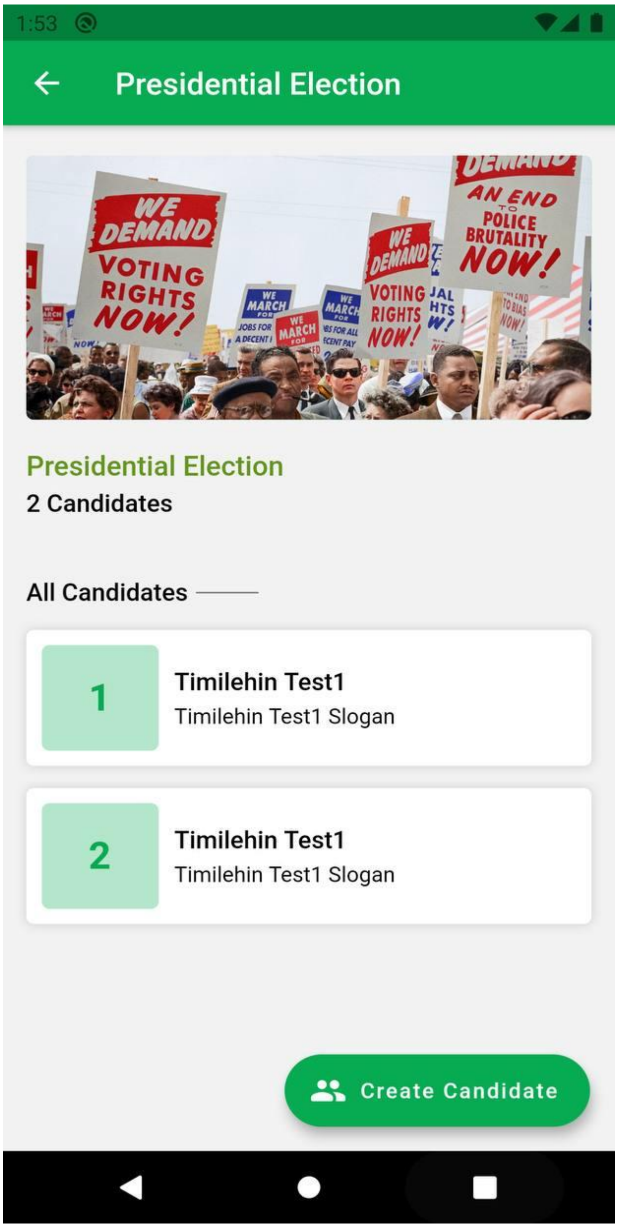


Figure 4.14: Admin Election Screen

4.2.8 Facial Verification Page

After login, the users (voters and admin) are required to verify their face to access the dashboard (Figure 4.15). The purpose of this page is to provide security for the users.

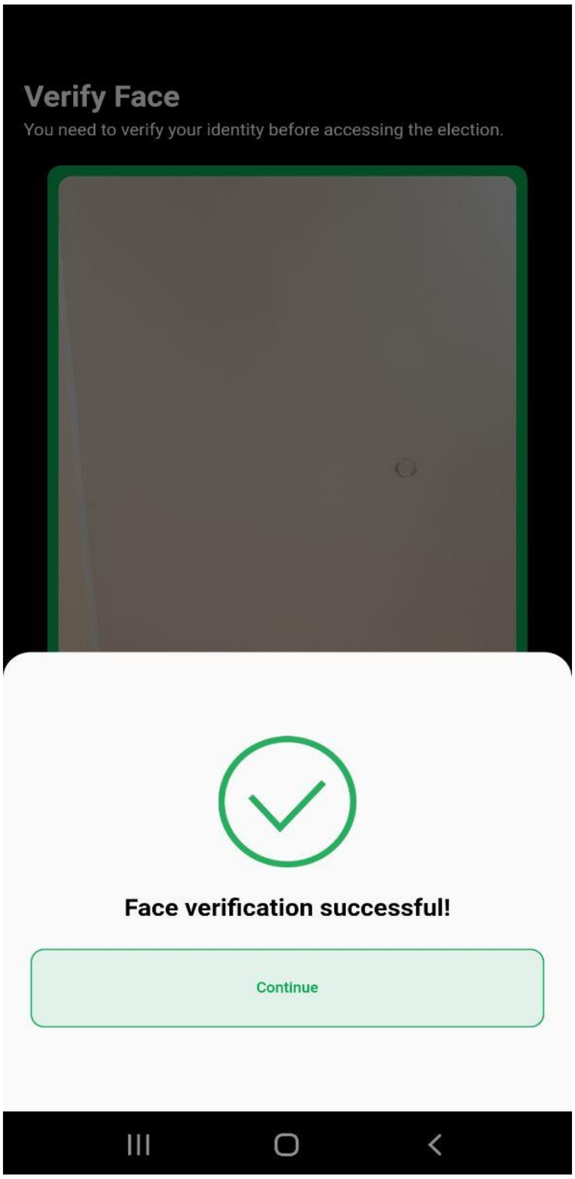


Figure 4.15: Facial verification page

4.2.9 Result Page

This is to check all the candidates for the post and their votes (Figure 4.16). The purpose of this page is to see the outcome of how the voting went and know the winner.

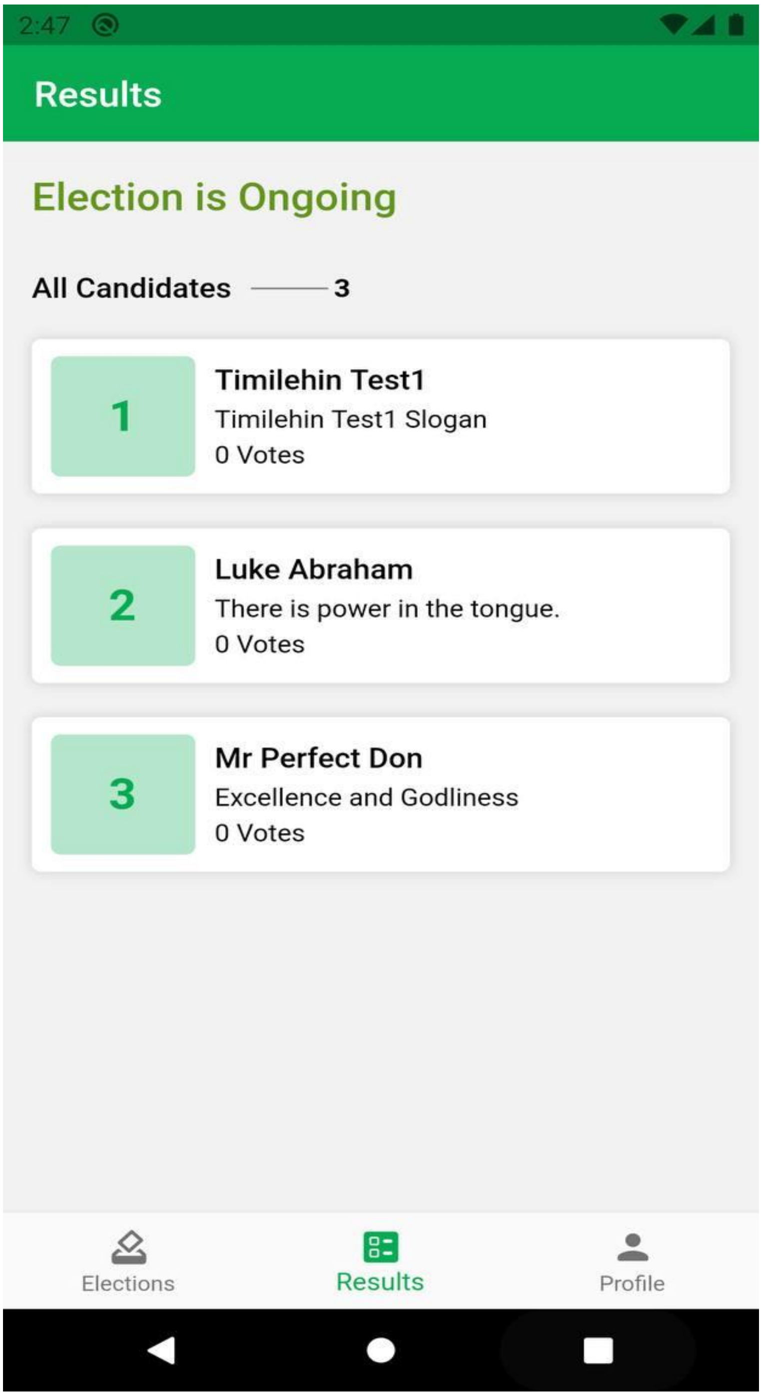


Figure 4.16: The Result Screen

4.3 THE ELECTION CONTRACT

This is the blockchain storage from Genache (Figure 4.17)

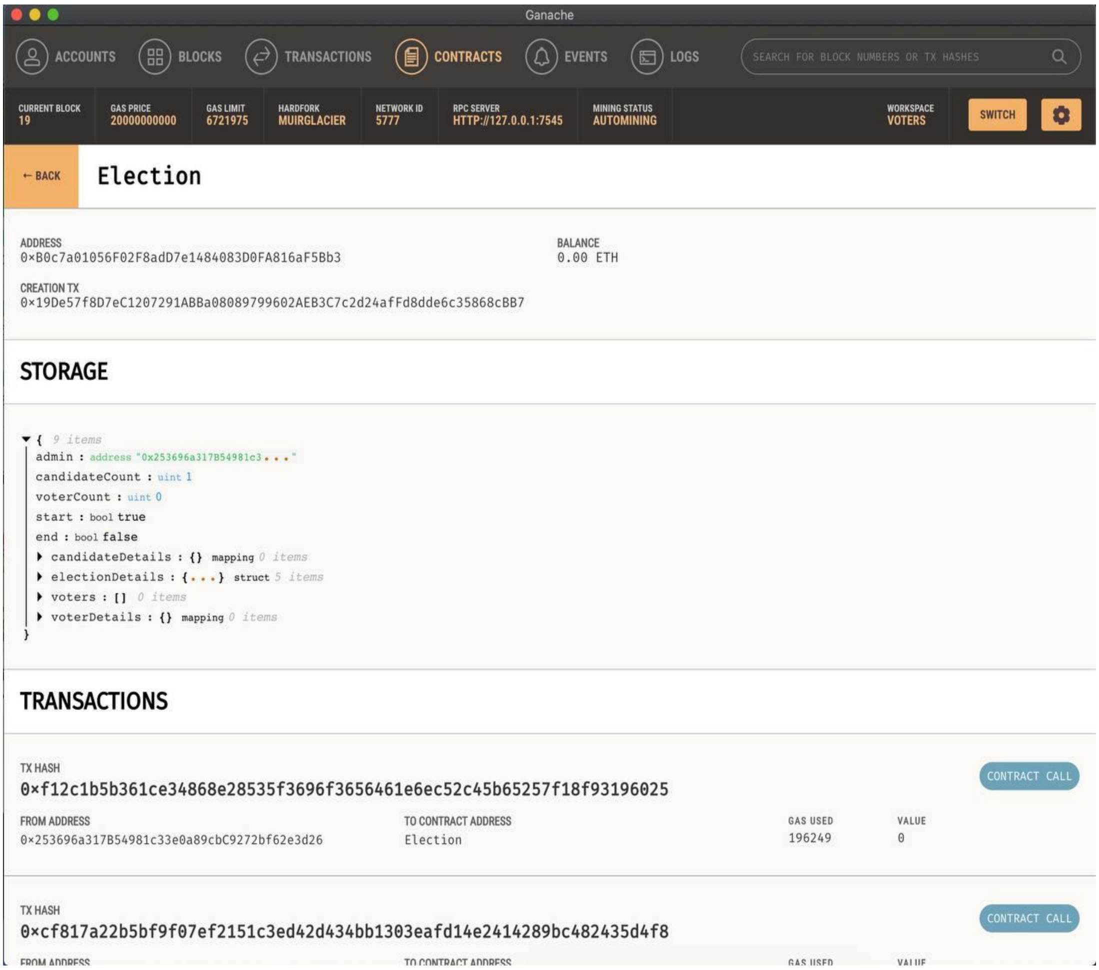


Figure 4.17: Blockchain Storage

The deployed Election contract from Genache (Figure 4.18)

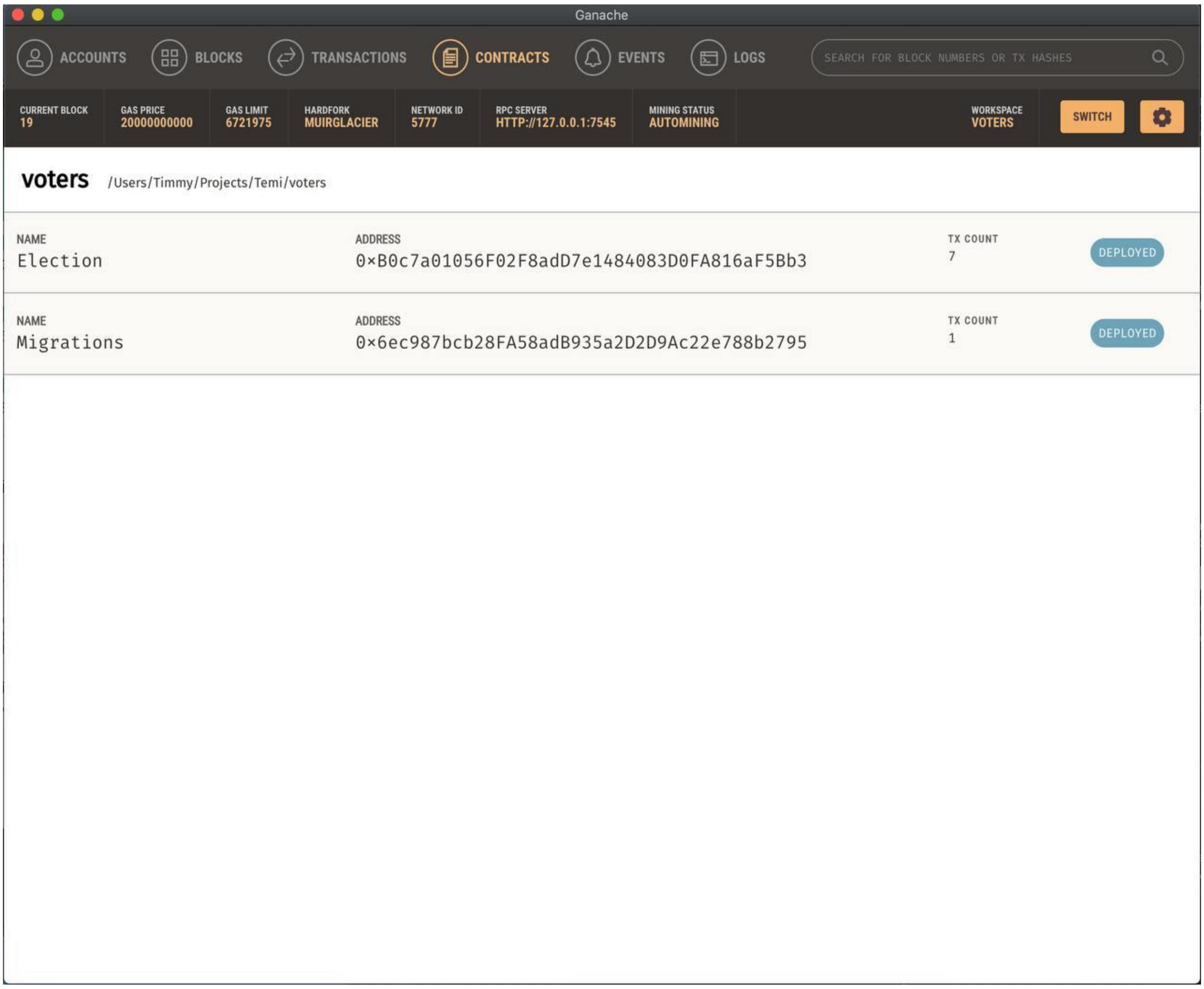


Figure 4.18: Deployed Contract

CHAPTER 5

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 SUMMARY

Current voting systems, like many aspects of industrial and governmental processes, is heavily outdated. Blockchain is a clear and obvious solution to many of the problems with the way we currently vote. The immutability, and transparency allows for voter anonymity while making it exceptionally difficult for any individuals or groups to illegally leverage control of an election. The use of smart contracts adds greater functionality and permits more voting options. In this way, once voting commences the added security layer using facial recognition would not significantly slow down the overall process as the contract would have been verified before the voting begins.

5.2 CONTRIBUTION TO KNOWLEDGE

The notable contribution of this project shows efficient and effective ways citizens can vote for their desired candidates from the comfort of their homes. It also increases voter's participation in the election of a country because of the transparent process.

5.3 CONCLUSION

The system developed encourages participation from citizens using Blockchain technology and verification of faces during election which has proved to be more convenient for counting votes and ensuring the process goes smoothly than the traditional methods.

5.4 RECOMMENDATION

Suggestions from the senior software engineer to improve the code quality with appropriate design pattern and code comments practices. Additional functionalities like the poll custom category, print vote results, live chat and presentation view can be undertaken as future enhancement.

REFERENCES

Ben, C., Rodney, M., & Hilary, U. (2019, February). *Nigerians cast ballots in delayed election after explosions, gunfire | PBS NewsHour Weekend*. https://www.pbs.org/newshour/world/nigerians-cast-ballots-in-delayed-election-after-explosions-gunfire

Benny, A. (2020). Blockchain based E-voting System. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3648870

Daramola, O., & Thebus, D. (2020). Architecture-centric evaluation of blockchain-based smart contract E-voting for national elections. *Informatics*, *7*(2), 16. https://doi.org/10.3390/informatics7020016

DataFlair. (2018). *Types of Blockchains - Decide which one is better for your Investment Needs - DataFlair*. https://data-flair.training/blogs/types-of-blockchain/

Early Card Punch Machines. (2021). http://www.columbia.edu/cu/computinghistory/oldpunch.html

Fusco, F., Lunesu, M. I., Pani, F. E., & Pinna, A. (2018). Crypto-voting, a blockchain based e-voting system. *IC3K 2018 - Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management*, *3*, 223–227. https://doi.org/10.5220/0006962102230227

Haber, S., & Stornetta, W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology*, *3*(2), 99–111. https://doi.org/10.1007/BF00196791

Hanifatunnisa, R., & Rahardjo, B. (2018). Blockchain based e-voting recording system design. *Proceeding of 2017 11th International Conference on Telecommunication Systems Services and Applications, TSSA 2017*, *2018-January*, 1–6. https://doi.org/10.1109/TSSA.2017.8272896

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockchain-Based E-Voting System. *IEEE International Conference on Cloud Computing, CLOUD*, *2018-July*, 983–986. https://doi.org/10.1109/CLOUD.2018.00151

Isirova, K., Kiian, A., Rodinko, M., & Kuznetsov, A. (2020). Decentralized electronic voting system based on blockchain technology developing principals. *CEUR Workshop Proceedings*, *2608*, 211–223.

Khan, K. M., Arshad, J., & Khan, M. M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research*, *14*(1), 53–62. https://doi.org/10.4018/IJEGR.2018010103

Liang, Y.-C. (2020, January). *1 The structure of a Blockchain. A block is composed of a header and a... | Download Scientific Diagram*. https://www.researchgate.net/figure/The-structure-of-a-Blockchain-A-block-is-composed-of-a-header-and-a-body-where-a-header_fig1_337306138

Mayhew, S. (2021). *History of Biometrics | Biometric Update*. https://www.biometricupdate.com/201802/history-of-biometrics-2

Mehboob Khan, K., Arshad, J., & Khan, M. M. (n.d.). *Secure Digital Voting System based on Blockchain Technology*.

Miller, S. (2020, February). *Online voting takes another hit -- GCN*. https://gcn.com/articles/2020/02/14/mit-voatz-voting-app-security.aspx

Mohammedali, N., & Al-Sherbaz, A. (2019). Election System Based on Blockchain Technology. *International Journal of Computer Science and Information Technology*, *11*(5), 13–31. https://doi.org/10.5121/ijcsit.2019.11502

Nakamoto, S. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org

Ndem, A. (2018). *Three risks posed by electronic voting - The Election Network*. http://theelectionnetwork.com/2018/10/25/three-risks-posed-by-electronic-voting/

ORACLE. (2015). *What Is a Database | Oracle*. Oracle. https://www.oracle.com/database/what-is-database/

Patil, H. V, Rathi, K. G., Tribhuwan, M. V, Science, C., & College, D. Y. P. A. C. S. (2018). A Study on Decentralized E-Voting System Using Blockchain Technology. *International Research Journal of Engineering and Technology (IRJET)*, *5*(11), 48–53. %0Awww.irjet.net

Prasetyadi, G. C., Mutiara, A. B., & Refianti, R. (2020). Blockchain-based electronic voting system with special ballot and block structures that complies with indonesian principle of voting. *International Journal of Advanced Computer Science and Applications*, *11*(1), 164–170. https://doi.org/10.14569/ijacsa.2020.0110121

Sadia, K., Masuduzzaman, M., Paul, R. K., & Islam, A. (2019). *Blockchain Based Secured E-voting by Using the Assistance of Smart Contract*. http://arxiv.org/abs/1910.13635

Sharma, K. K., Raghatwan, J., Patole, M., & Lomte, V. M. (2019). Voting system using multichain blockchain and fingerprint verification. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 3588–3597. https://doi.org/10.35940/ijitee.A4170.119119

StudyTonight. (2020). *DBMS Tutorial | Studytonight*. https://www.studytonight.com/dbms/

Suganya, R., Sureshkumar, A., Alaguvathana, P., Priyadharshini, S., & Jeevanantham, K. (2020). Blockchain Based Secure Voting System Using Iot. *International Journal of Future Generation Communication and Networking*, *13*(3), 2134–2142. http://www.sersc.org/journals/index.php/IJFGCN/article/view/28815

Techopedia. (2016). *What is a File System? - Definition from Techopedia*. https://www.techopedia.com/definition/5510/file-system

Thales. (2021). *Facial Recognition in 2021 (with examples)*. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

Vaishnavi, M. R. (2020). *What is a Database? Know the Definition, Types & Components | Edureka*. https://www.edureka.co/blog/what-is-a-database/

VerifiedVoting. (2020). *Voting Equipment – Verified Voting*. https://verifiedvoting.org/votingequipment/

Voting Equipment – Verified Voting. (2020). https://verifiedvoting.org/votingequipment/

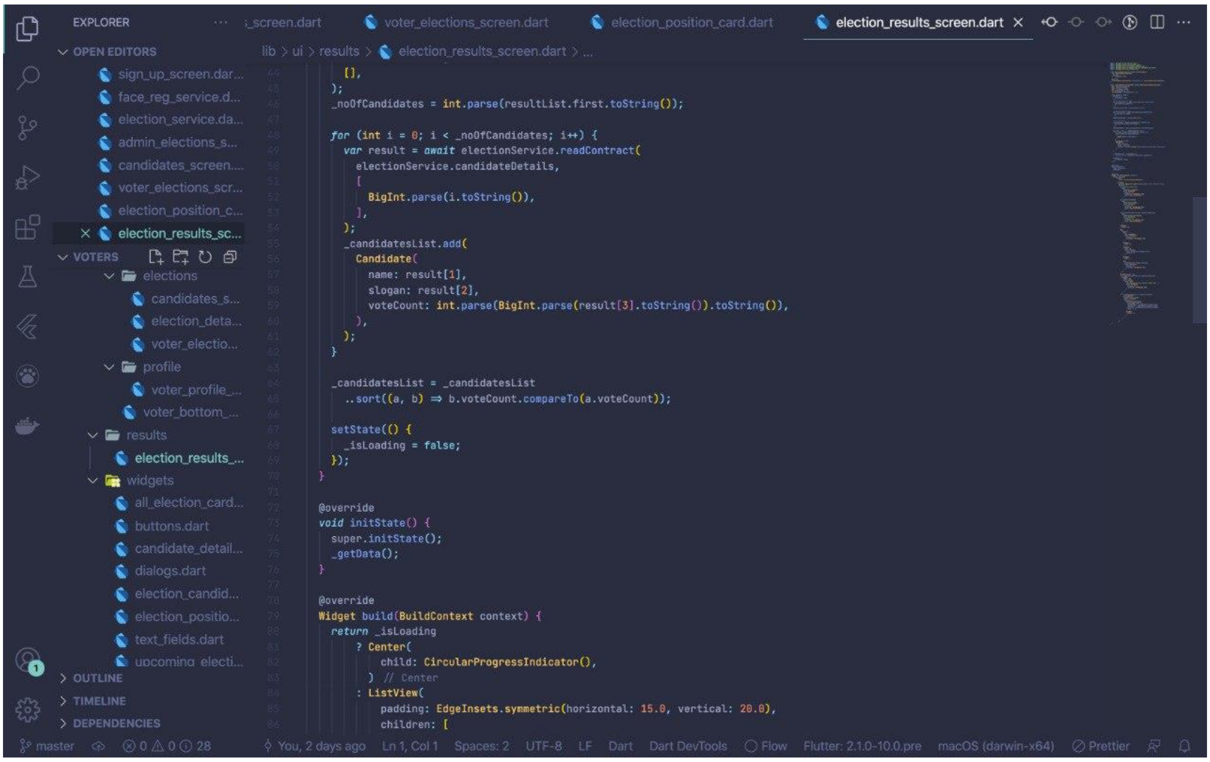
Voting Machines - Elections - Ballots - Politics - The New York Times. (2008). https://www.nytimes.com/2008/01/06/magazine/06Vote-t.html

Wei, C. C. Z., & Wen, C. C. (2018). Blockchain-based electronic voting protocol. *International Journal on Informatics Visualization*, *2*(4–2), 336–341. https://doi.org/10.30630/joiv.2.4-2.174

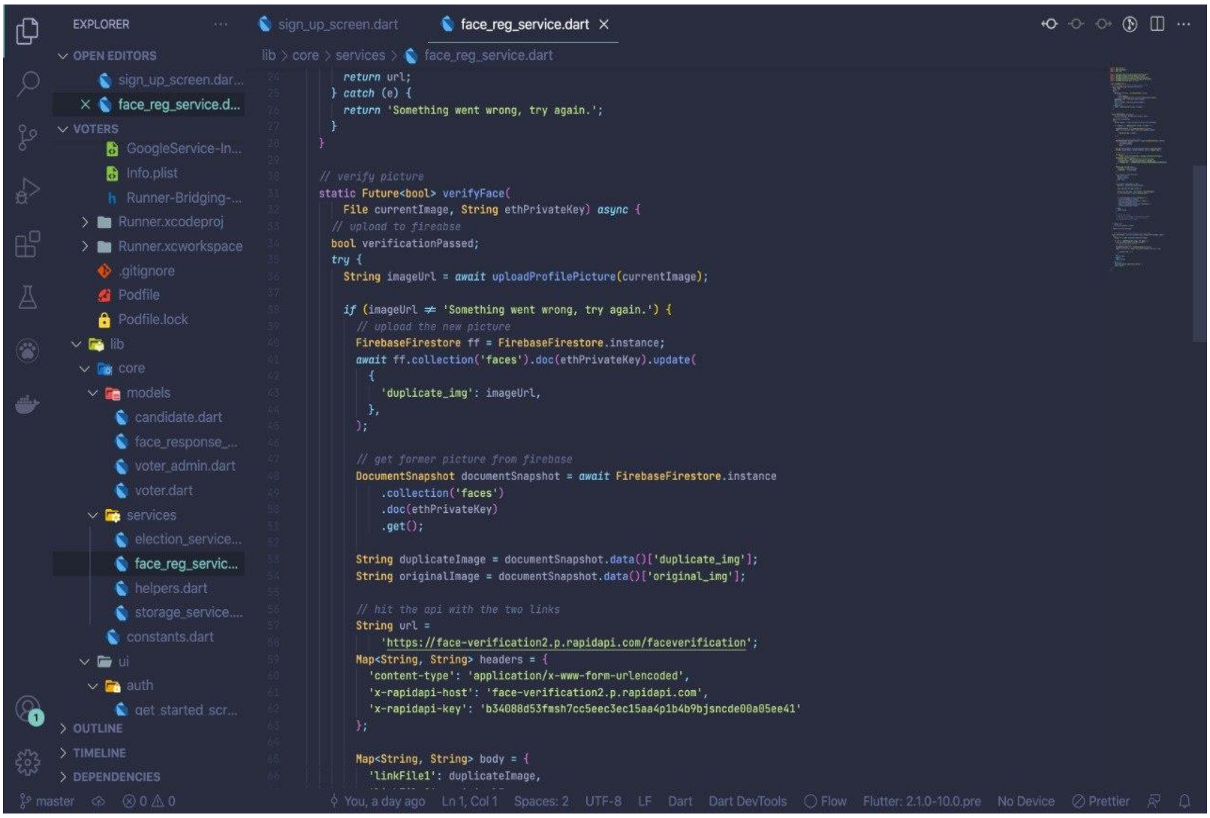
Wikipedia. (2021, August). *Elections in Nigeria - Wikipedia*. https://en.wikipedia.org/wiki/Elections_in_Nigeria

Yi, H. (2019). Securing e-voting based on blockchain in P2P network. *Eurasip Journal on Wireless Communications and Networking*, *2019*(1). https://doi.org/10.1186/s13638-019-1473-6

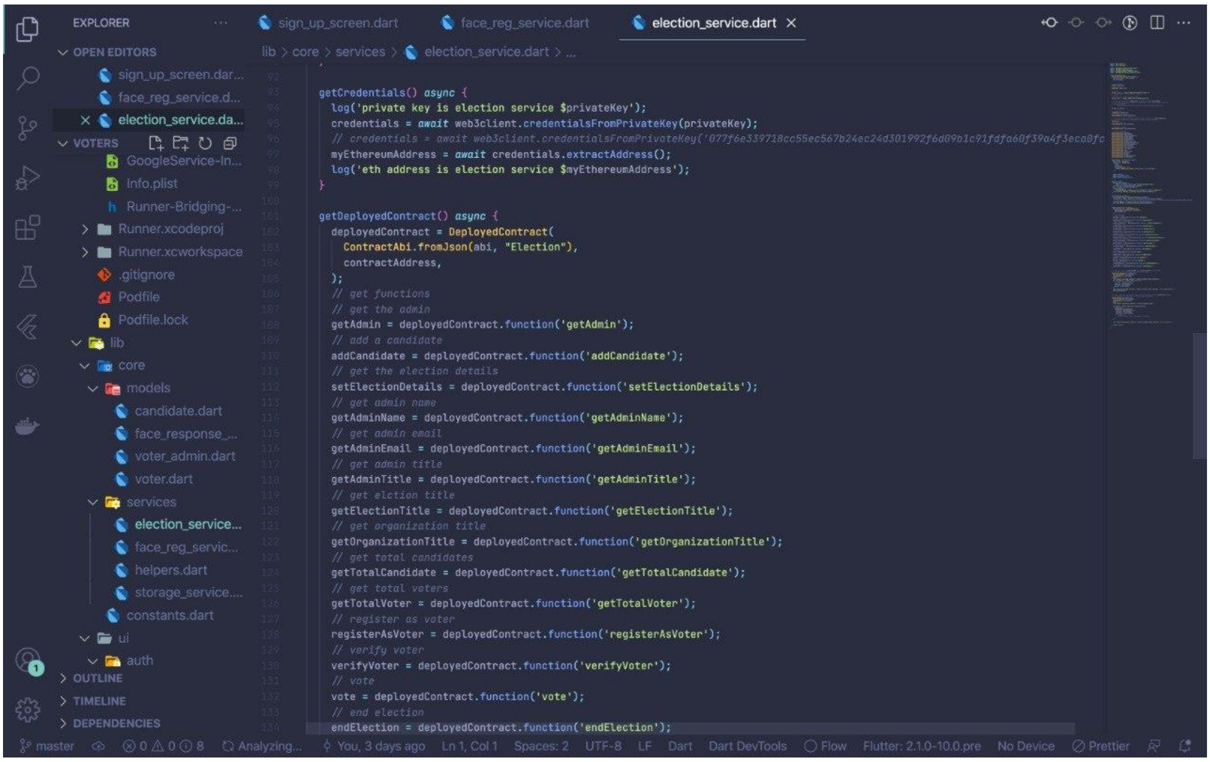
APPENDIX



APPENDIX A

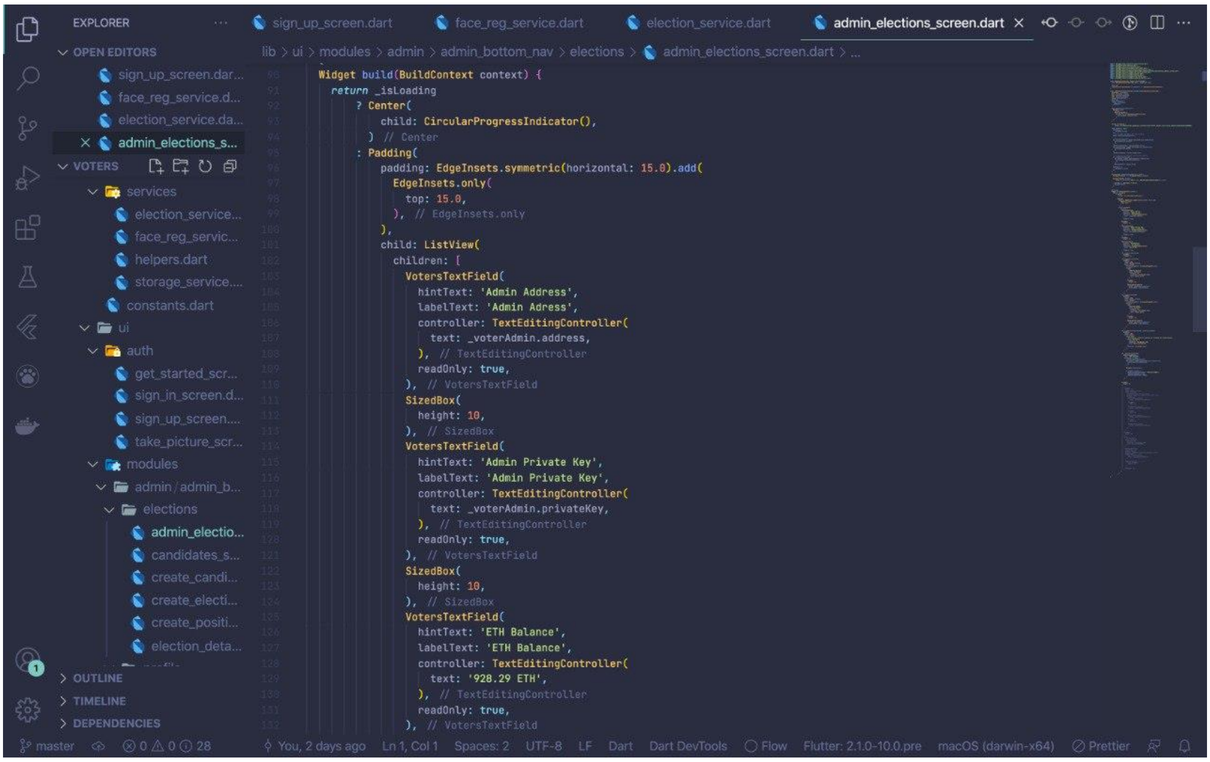

sign_up_screen.dart
face_reg_service.dart
lib > core > services > face_reg_service.dart
return url;
} catch (e) {
return 'Something went wrong, try again.';
}
}
// verify picture
static Future<bool> verifyFace(
File currentImage, String ethPrivateKey) async {
// upload to fireabse
bool verificationPassed;
try {
String imageUrl = await uploadProfilePicture(currentImage);
if (imageUrl != 'Something went wrong, try again.') {
// upload the new picture
FirebaseFirestore ff = FirebaseFirestore.instance;
await ff.collection('faces').doc(ethPrivateKey).update(
{
'duplicate_img': imageUrl,
},
);
// get former picture from firebase
DocumentSnapshot documentSnapshot = await FirebaseFirestore.instance
.collection('faces')
.doc(ethPrivateKey)
.get();
String duplicateImage = documentSnapshot.data()['duplicate_img'];
String originalImage = documentSnapshot.data()['original_img'];
// hit the api with the two links
String url =
'https://face-verification2.p.rapidapi.com/faceverification';
Map<String, String> headers = {
'content-type': 'application/x-www-form-urlencoded',
'x-rapidapi-host': 'face-verification2.p.rapidapi.com',
'x-rapidapi-key': 'b34088d53fmsh7cc5eec3ec15aa4p1b4b9bjsncde00a05ee41'
};
Map<String, String> body = {
'linkFile1': duplicateImage,
You, a day ago Ln 1, Col 1 Spaces: 2 UTF-8 LF Dart Dart DevTools Flow

APPENDIX B

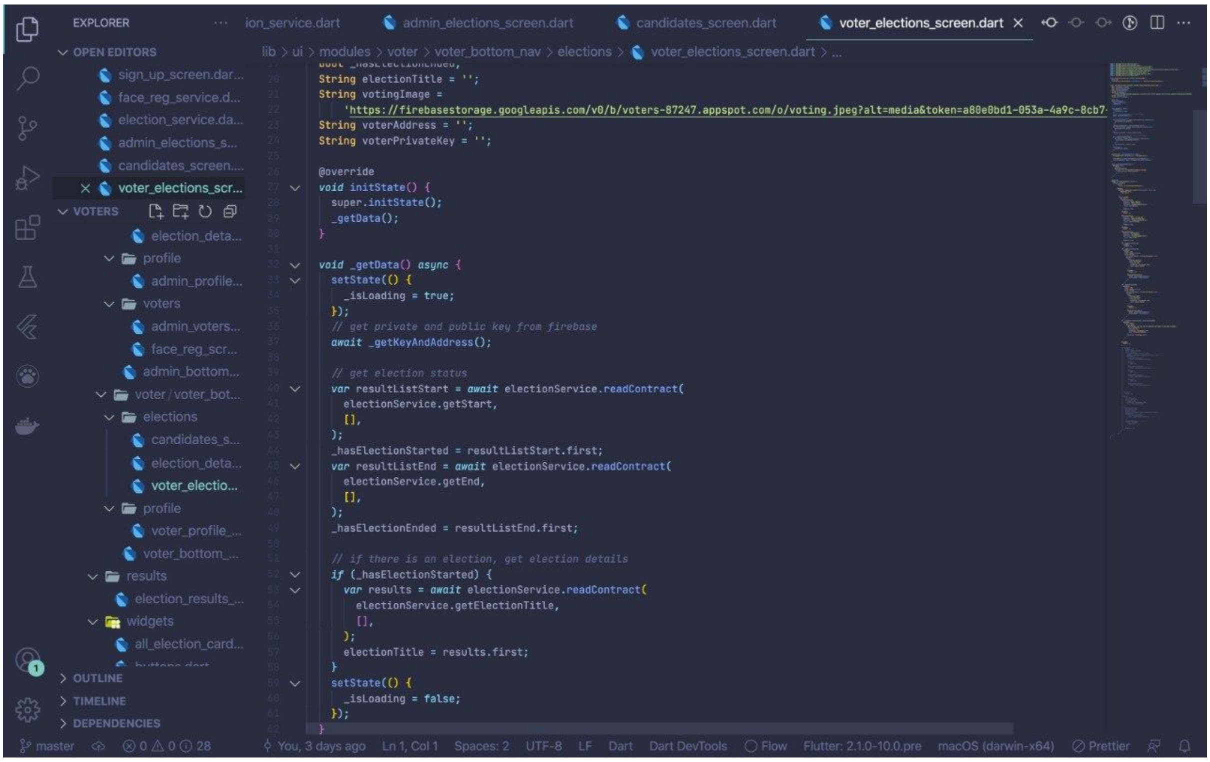


sign_up_screen.dart
face_reg_service.dart
election_service.dart
lib > core > services > election_service.dart > ...
getCredentials() async {
log('private key is election service $privateKey');
credentials = await web3client.credentialsFromPrivateKey(privateKey);
myEthereumAddress = await credentials.extractAddress();
log('eth address is election service $myEthereumAddress');
}
getDeployedContract() async {
deployedContract = DeployedContract(
ContractAbi.fromJson(abi, "Election"),
contractAddress,
);
// get functions
// get the admin
getAdmin = deployedContract.function('getAdmin');
// add a candidate
addCandidate = deployedContract.function('addCandidate');
// get the election details
setElectionDetails = deployedContract.function('setElectionDetails');
// get admin name
getAdminName = deployedContract.function('getAdminName');
// get admin email
getAdminEmail = deployedContract.function('getAdminEmail');
// get admin title
getAdminTitle = deployedContract.function('getAdminTitle');
// get elction title
getElectionTitle = deployedContract.function('getElectionTitle');
// get organization title
getOrganizationTitle = deployedContract.function('getOrganizationTitle');
// get total candidates
getTotalCandidate = deployedContract.function('getTotalCandidate');
// get total voters
getTotalVoter = deployedContract.function('getTotalVoter');
// register as voter
registerAsVoter = deployedContract.function('registerAsVoter');
// verify voter
verifyVoter = deployedContract.function('verifyVoter');
// vote
vote = deployedContract.function('vote');
// end election
endElection = deployedContract.function('endElection');

APPENDIX C

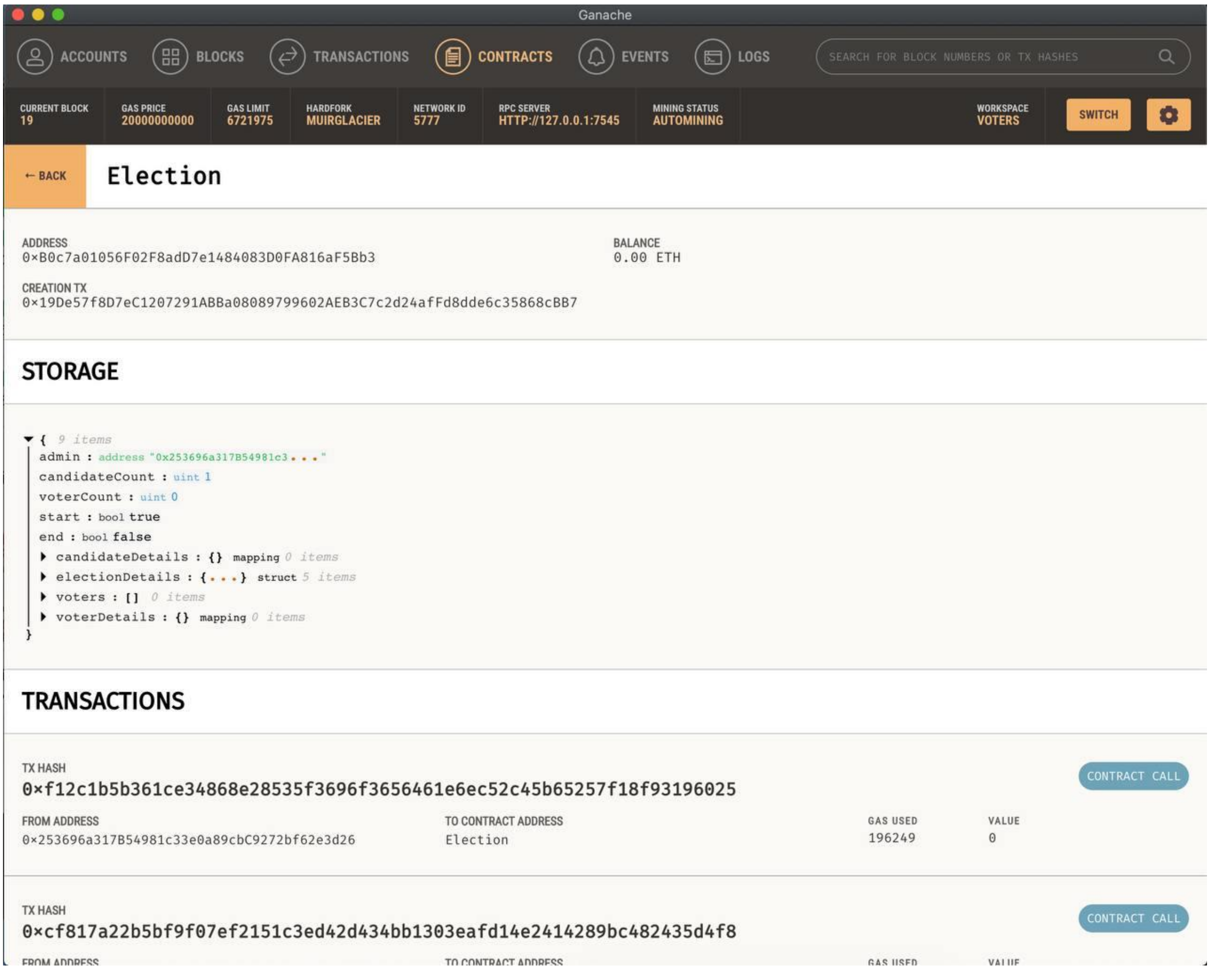

EXPLORER
sign_up_screen.dart
face_reg_service.dart
election_service.dart
admin_elections_screen.dart
lib > ui > modules > admin > admin_bottom_nav > elections > admin_elections_screen.dart > ...
OPEN EDITORS
VOTERS
services
helpers.dart
constants.dart
ui
auth
modules
elections
OUTLINE
TIMELINE
DEPENDENCIES
Widget build(BuildContext context) {
return _isLoading
? Center(
child: CircularProgressIndicator(),
) // Center
: Padding(
padding: EdgeInsets.symmetric(horizontal: 15.0).add(
EdgeInsets.only(
top: 15.0,
), // EdgeInsets.only
),
child: ListView(
children: [
VotersTextField(
hintText: 'Admin Address',
labelText: 'Admin Adress',
controller: TextEditingController(
text: _voterAdmin.address,
), // TextEditingController
readOnly: true,
), // VotersTextField
SizedBox(
height: 10,
), // SizedBox
VotersTextField(
hintText: 'Admin Private Key',
labelText: 'Admin Private Key',
controller: TextEditingController(
text: _voterAdmin.privateKey,
), // TextEditingController
readOnly: true,
), // VotersTextField
SizedBox(
height: 10,
), // SizedBox
VotersTextField(
hintText: 'ETH Balance',
labelText: 'ETH Balance',
controller: TextEditingController(
text: '928.29 ETH',
), // TextEditingController
readOnly: true,
), // VotersTextField
master
You, 2 days ago Ln 1, Col 1 Spaces: 2 UTF-8 LF Dart Dart DevTools Flow Flutter: 2.1.0-10.0.pre macOS (darwin-x64) Prettier

APPENDIX D



voter_elections_screen.dart
lib > ui > modules > voter > voter_bottom_nav > elections > voter_elections_screen.dart > ...
String electionTitle = '';
String votingImage =
'https://firebasestorage.googleapis.com/v0/b/voters-87247.appspot.com/o/voting.jpeg?alt=media&token=a80e0bd1-053a-4a9c-8cb7
String voterAddress = '';
String voterPrivateKey = '';
@override
void initState() {
super.initState();
_getData();
}
void _getData() async {
setState(() {
_isLoading = true;
});
// get private and public key from firebase
await _getKeyAndAddress();
// get election status
var resultListStart = await electionService.readContract(
electionService.getStart,
[],
);
_hasElectionStarted = resultListStart.first;
var resultListEnd = await electionService.readContract(
electionService.getEnd,
[],
);
_hasElectionEnded = resultListEnd.first;
// if there is an election, get election details
if (_hasElectionStarted) {
var results = await electionService.readContract(
electionService.getElectionTitle,
[],
);
electionTitle = results.first;
}
setState(() {
_isLoading = false;
});
}

APPENDIX E


Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 19
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE VOTERS
SWITCH
← BACK
Election
ADDRESS
0×B0c7a01056F02F8adD7e1484083D0FA816aF5Bb3
BALANCE
0.00 ETH
CREATION TX
0×19De57f8D7eC1207291ABBa08089799602AEB3C7c2d24afFd8dde6c35868cBB7
STORAGE
{ 9 items
admin : address "0x253696a317B54981c3..."
candidateCount : uint 1
voterCount : uint 0
start : bool true
end : bool false
candidateDetails : {} mapping 0 items
electionDetails : {...} struct 5 items
voters : [] 0 items
voterDetails : {} mapping 0 items
}
TRANSACTIONS
TX HASH
0×f12c1b5b361ce34868e28535f3696f3656461e6ec52c45b65257f18f93196025
CONTRACT CALL
FROM ADDRESS
0×253696a317B54981c33e0a89cbC9272bf62e3d26
TO CONTRACT ADDRESS
Election
GAS USED
196249
VALUE
0
TX HASH
0×cf817a22b5bf9f07ef2151c3ed42d434bb1303eafd14e2414289bc482435d4f8
CONTRACT CALL

APPENDIX F