**A Project Report on**

# “E-VOTING BASED ON AADHAR USING BLOCKCHAIN TECHNOLOGY”

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE

IN THE PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE AWARD OF THE DEGREE

OF

BACHELOR OF ENGINEERING (INFORMATION TECHNOLOGY ENGINEERING)

(Academic Year: 2021-22)

*SUBMITTED BY*

|  |  |
| --- | --- |
| **Mr. Ameya Vijaysingh Lodhavat** | **(Exam Seat No: B150478531)** |
| **Mr. Vivek Bidgar** | **(Exam Seat No: B150478510)** |
| **Mr. Kunal Patil** | **(Exam Seat No: B150478545)** |
| **Ms.Rinku Jadhav** | **(Exam Seat No: B150478565)** |

*Under the guidance of*

**Ms. Kanchan Dhomse**

DEPARTMENT OF INFORMATION TECHNOLOGY ENGINEERING



MET’s Institute of Engineering,

Adgaon, Nashik-422003

SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE

May, 2022



# *Certificate*

*This is to Certify that the project report entitles*

## “MET’s Institute of Engineering”

|  |  |
| --- | --- |
| **Mr. Ameya Vijaysingh Lodhavat** | **(Exam Seat No:B150478531)** |
| **Mr. Vivek Bidgar** | **(Exam Seat No:B150478510)** |
| **Mr. Kunal Patil** | **(Exam Seat No:B150478545)** |
| **Ms . Rinks Jadhav** | **(Exam Seat No:B150478565)** |

*are bonafide students of this institute and the work has been carried out by them under the guidance of Ms. Kqnchan Dhomse and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University for the award of the degree of Bachelor of Engineering (Information Technology Engineering).*

Project Guide H.O.D Principal

(Ms. Kanchan Dhomse) (Dr. S.V.Gumaste) (Dr. V. P. Wani)

Date: / /

# Acknowledgements

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individual and organizations. We would like to extend our sincere thanks to all of them. It gives us proud privilege to complete the project on **“E-VOTING BASED ON AADHAR USING BLOCKCHAIN TECHNOLOGY”**. We are highly indebted to our internal guide **Ms. Madhuri Shinde** for her guidance and constant supervision as well as for providing necessary information regarding the project and also for her support in completing the project.

We are also extremely grateful to our respected H.O.D. (Computer Department) **Dr. M. U. Kharat** and **Prof. Priti Metange** (Project Co-ordinator) for

providing all facilities and every help for smooth progress of project work.

Our thanks and appreciation also goes to our beloved parents for their blessings, all the staff members, friends and colleagues for providing help and support in our work.

Mr. Ameya Vijaysingh Lodhavat

Mr. Vivek Bidgar

Mr. Kunal Patil

Ms. Rinks Jadhav

# Abstract

This system allows people to vote electronically in public elections with a security system using block chain technology. Progressively, the application of scientific knowledge for practical purposes within the concept aids in the survival of many people. This methodology sets out an Associate in legal organisation for native election on blockchain knowledge dealing with applied sciences and Aadhar affirmation. Being free of threat and dispositive may be a risk of extensive election using this prevalent methodology. A number of issues that may persist within the prevailing methodology are with a corporation that has management over the information. It can be done to meddle with the information for a good time. The projected methodology is principally designed for our native-supported Aadhar affirmation. A single system will act as both a registering module and a voting module. The system will act as a registering module on activation of the switch by the super admin. The QR code of Aadhar is scanned, where block chain technology comes into existence and is integrated within the machine. Each vote is added to each block encrypted by 256-bit SHA hash codes. The hashed block cannot be tampered with by any individual as more security is added to the system. By incorporating Blockchain into information distribution, one of the cheating sources of database manipulation will be reduced.

# Contents

1. **Introduction 1**
   1. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2
2. **Literature Survey 3**
   1. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4
3. **Architecture 5**
   1. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
4. **Proposed System 7**
   1. Advantages Of The Proposed System . . . . . . . . . . . . . . . . . . 8
   2. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
5. **Module Description 9**
   1. Voter Module . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
   2. Election Commission Module . . . . . . . . . . . . . . . . . . . . . . 9
   3. Blockchain Module . . . . . . . . . . . . . . . . . . . . . . . . . . . 10
   4. Pre-Registration Of User . . . . . . . . . . . . . . . . . . . . . . . . 11
   5. Process of Voting . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11
   6. Hashing of Blocks in Blockchain . . . . . . . . . . . . . . . . . . . . 12
   7. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14
6. **Blockchain Technology and Its Working 15**
   1. Blockchain Technology . . . . . . . . . . . . . . . . . . . . . . . . . 15
   2. Popularity of Blockchain . . . . . . . . . . . . . . . . . . . . . . . . 16
   3. Working of Blockchain . . . . . . . . . . . . . . . . . . . . . . . . . 17
   4. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 17

E-Voting Based on Aadhar Using Blockchain Technology

1. **Types of Blockchain 18**
   1. Private Blockchain Networks . . . . . . . . . . . . . . . . . . . . . . 18
   2. Public Blockchain Networks . . . . . . . . . . . . . . . . . . . . . . 18
   3. Permissioned Blockchain Networks . . . . . . . . . . . . . . . . . . . 19
   4. Consortium Blockchains . . . . . . . . . . . . . . . . . . . . . . . . 19
   5. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 19
2. **Properties of Blockchain E-Voting System Using Vid 20**
   1. Authentication . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 20
   2. Availability . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 20
   3. Publicly Verifiable . . . . . . . . . . . . . . . . . . . . . . . . . . . 20
   4. Integrity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
   5. Sha Algorithm . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
   6. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 21
3. **Testing 22**
   1. Formal Technical Review . . . . . . . . . . . . . . . . . . . . . . . . 22
   2. Test Plan . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22
   3. Publicly Verifiable . . . . . . . . . . . . . . . . . . . . . . . . . . . 23
   4. Integrity . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
   5. Sha Algorithm . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24
   6. Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 24

**10App Layout 25**

**11Firebase Cloud 27**

11.1 Summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 29

**12Conclusion 30**

**Bibliography 31**

MET’s Institute of Engineering iv

# List of Figures

|  |  |
| --- | --- |
| 1.1 Introduction . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 1 |
| 3.1 System Architecture . . . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
| 5.1 User Registration . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 11 |
| 5.2 OTP service and authentication services by UIDAI. . . . . . . . . . . . | 12 |
| 5.3 3-Figure5-1 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 13 |
| 5.4 Hash Function . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 14 |
| 10.1 Registration-Login Interface . . . . . . . . . . . . . . . . . . . . . . | 25 |
| 10.2 Admin Interface . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 26 |
| 11.1 Real time database 1 . . . . . . . . . . . . . . . . . . . . . . . . . . | 28 |
| 11.2 Real Time Database 2 . . . . . . . . . . . . . . . . . . . . . . . . . | 28 |

v

# List of Tables

2.1 Literature Survey . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

9.1 Test Plan for E-voting based on Aadhar using blockchain technology . . 23

vi

**Chapter 1**

# Introduction

The scientific knowledge that has been used for a practical purpose has become a daily routine at this time to fulfil our needs. It has created a new barrier within the



Figure 1.1: Introduction

method of practical principles of social equality in general. nowadays has no belief in their administration, making elections momentous in a very trendy social equality society.

The election is currently active and needs a physical enrolment with a citizen identity. The citizen will initiate the formal decision of a choice only if they supply the citizen’s identity. The foremost downside of choosing a formal decision is the counterfeit poll. To overcome the difficulties, our proposed system tends to use several methods of approving unique standards. For each government process to be performed, it needs the identity card supplied with identification that gives no doubt that the citizen has all the rights to execute the specified activity. The projected information makes less the complete authorization within the small temporary tent and, consequently, makes less the person employed in the investigation method.

## 1.1 Summary

In this chapter we are mainly focusing on using VID of the Aadhar which allows the service providers to make verification.

**Chapter 2**

# Literature Survey

Table 2.1: Literature Survey

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Year** | **Author** | **Objective** | **Methodology** | **Observation** |
| 2016 | S. Hof | In his research, using diverse scientific analysis of biological data in voting and their state of being free from danger, were examined. | He discussed the self-indulgent liking for scientific analysis methodology, such as the trick played by something, not taking on and dismissing quantity, etc. |  |
| 2017 | S. M.  Hasan | A representation of the device with micro-chips where citizen affirmation was executed using identity module verification. |  | Several polls in this series were hampered by an aspect of performance in this card after the citizen had stopped his ballot at phase. |
| **Year** | **Author** | **Objective** | **Methodology** | **Observation** |
| 2017 and  2016 | N. S.  Tilwani  and R. M.  Prasad | A composition that is related to or based on a ballot arrangement was proposed. |  |  |
|  | Khasawneh | To overcome the problem by using block chain technology to increase security and prevent vote theft. | A network methodology thought with joined or merged scientific analysis of biological data substantiated as an impression, aperture forecasting, and so on. |  |

## 2.1 Summary

In this chapter, the Literature survey provide us the information regrading in development in voting system along with security and privacy using blockchain over a period of time.

**Chapter 3**

# Architecture

Architecture In our model, we use the UIDAI’s Aadhaar, which is a unique ID generated for every registered citizen of India, as a private key, along with the public key assigned to an election for the purpose of voting. This, along with the vote of the

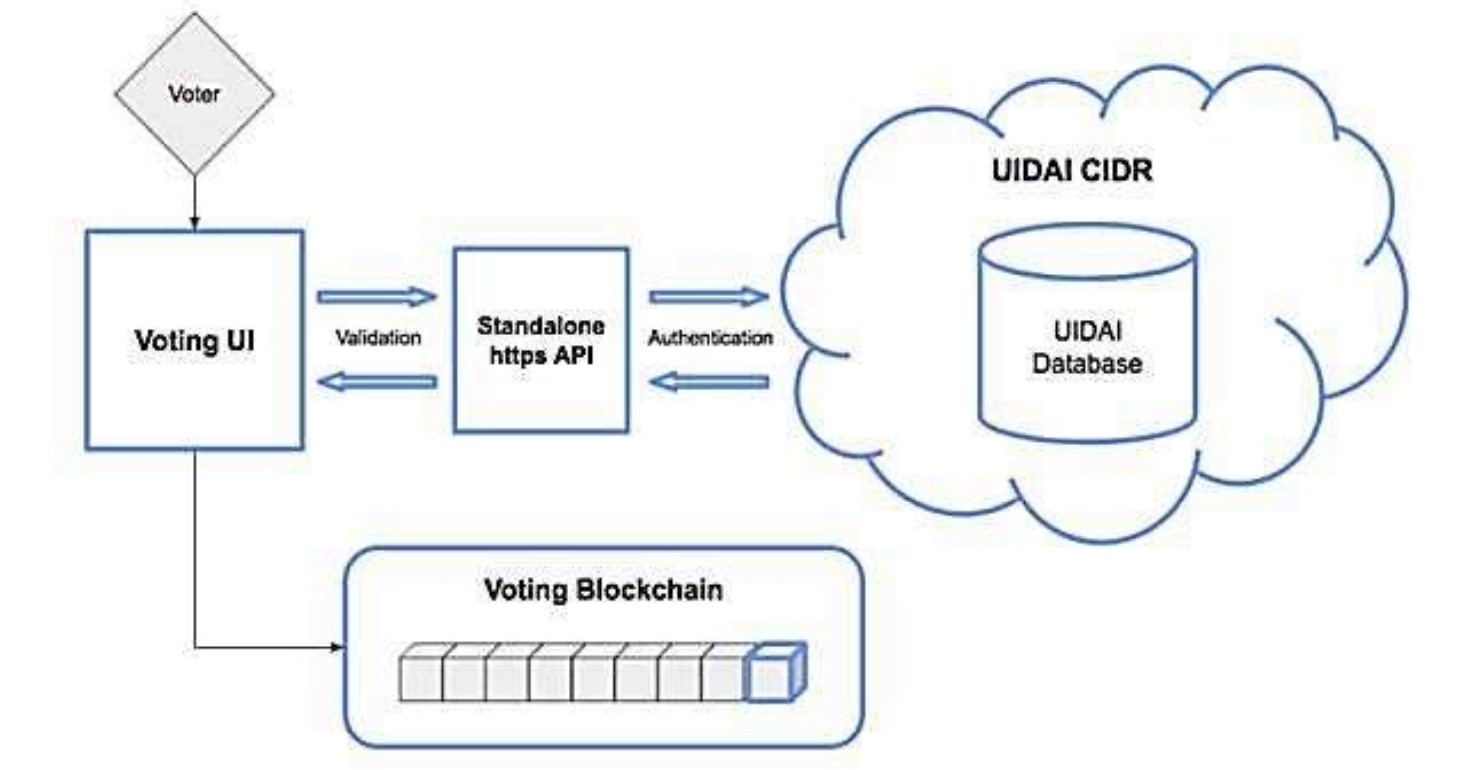


Figure 3.1: System Architecture

individual, is then used to generate a hash used to reserve/block the vote for that particular individual. The voting mechanism will take place over a government authorised portal (web/mobile) and the votes will be captured on a tamperproof instance available openly for the public to verify and validate. The SHA-256 algorithm is used to generate the hash for the next block as well as the encryption of the user’s identifiable data. The entire system rests on a standalone blockchain powered by cloud infrastructure. The proof-of-concept protocol is used for consensus on the blockchain.

## 3.1 Summary

In this chapter,UIDAI plays an important role to generate block using SHA-256 which is then updated to blockchain in Firebase Cloud.here proof-of-concept protocol is used for consensus of the blockchain.

**Chapter 4**

# Proposed System

In our system, the election commission board is set under the registration process in server. In the registration process, the new voter can register their ID for voting. When the election commission selects the voting progress in the server during the voting process, This is the time a voter can poll their vote. When the election commission deselects, the voting progress in the server is closed. The e-voting machine assigned as voting is closed at this time. Voters cannot be able to poll their vote. Finally, the election commission selects the result announcement option in the server, at this time, the election commission will start to count the votes automatically and announce the result. The proposed system is used for dual purposes:

1. Enrollment
2. Polling

In the server application, our proposed system builds four methods to improve the voting performance and reduce the manual process and manpower. The four methods are:

1. Under registration
2. voting progress
3. Voting closed
4. The Result announcement

As a way to fulfil the protection and security prerequisites for e-voting a ballot, and to guarantee that the political race system ought not to empower constrained voting, voters should cast a ballot in a regulated situation. In our work, a hyperledger private blockchain is arranged to accomplish these objectives. It uses a calculation that conveys similarly quick exchanges through an agreement instrument dependent on the way of life as a stake. It explains the background of the use of hyperledger for the blockchain system. Speak to each voter about a ballot locale. Each locale hub has a product specialist that self-sufficiently interfaces with the ”boot node” and deals with the existence pattern of the keen agreement on that hub. When the political race head makes a political decision, a voting form of keen agreement is circulated and conveyed to its relating locale hub. When the polling form shrewd agreements are made, every one of the comparing locale hubs is offered authorization to associate with their corresponding contract. At the point when an individual voter makes her choice from her related savvy contract, the vote information is confirmed by most of the comparing area hubs, and each vote they concede to is attached to the blockchain. The political decision process has the accompanying jobs:

1. Political decision-maker: To manage the lifecycle of a political campaign.Differentorganisations and organisations might be joined up with this job. The political decision managers make the political decision, register voters, choose the lifetime of the political decision, and appoint permissioned hubs.
2. A voter is a person who is qualified to cast a ballot. Voters can confirm themselves,load political race voting forms, make their choice and check their vote after a political decision is finished.

## 4.1 Advantages Of The Proposed System

1)Greater straightforwardness because of open and dispersed records,

2) Security and unwavering quality

## 4.2 Summary

The voting system uses adhar address for registration because of which it becomes easy to manage and access data easily as well the whole process from registration to casting vote becomes more efficient and secure with atmost privacy.

**Chapter 5**

# Module Description

## 5.1 Voter Module

At this stage, the voting of the considerable number of keys held by the voters has started, with the voters expecting that all the keys of the panel and witness have been raised before this stage starts. Here is an outline at this stage. This stage is the phase that will be passed by the voters as the political race happens. Starting with entering the terminal and ending with the terminal where the political decision is made. Voters will get a vacant polling form from the council which must be decoded by their particular voter private key. After the choice procedure is finished, it will consequently frame a progression of information that has a structure. The finish of this political race process is that each voter will get a hash that can be utilised if a voter needs to check the aftereffects of the political race. It is normal that every determination terminal doesn’t have a similar hash incentive for various voters.

## 5.2 Election Commission Module

Identifying a shrewd agreement incorporates three sections:

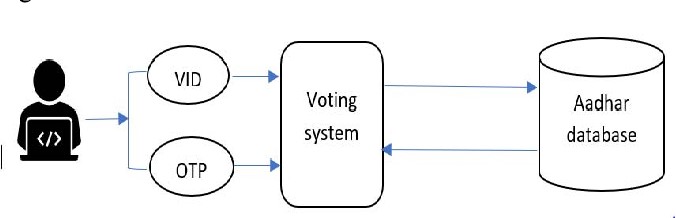
1. recognising the jobs that are associated with the understanding (the political race understanding for our situation),
2. the understanding procedure (i.e., political decision procedure), and
3. the exchanges (i.e., voting a ballot exchange) utilised in the savvy contract. 1) Election Jobs: The jobs in a keen agreement incorporate the gatherings that need to take an interest in understanding. The political race process has the accompanying jobs:(I) Election overseer: Handles the lifecycle of a political campaign. Numerous foundations and organisations believed they might be linked up with this job. Political race leaders make political decisions, register voters, determine the lifespan of political decisions, and relegate permissioned hubs. Political race heads make political decision polling forms utilising a keen agreement wherein the chairman characterises a rundown of possibilities for each vote in a ballot area. The savvy contracts are then composed onto the block chain, where area hubs’ access connects with their corresponding brilliant agreements.

## 5.3 Blockchain Module

E-Cryptography is the methodology for veiling and revealing, additionally called scrambling and unscrambling, information through complex number-crunching. This suggests the e-voting ballot voter information must be seen by the arranged recipients and nobody else. The strategy incorporates taking decoded data, for instance, voting a ballot data, and encoding it using a logical estimation, known as a figure. This conveys a ciphertext, a piece of e-voting a ballot information that is absolutely useless and unusual until it is decoded. This system for encryption is known as symmetric key cryptography. Blockchain advancement utilizes cryptography as techniques for ensuring exchanges of e-voting a ballot are done safely, while confirming all e-voting a ballot information and reserves of critical worth. Thusly, anyone using blockchain can have complete assurance that once e-voting a ballot information is recorded on a blockchain, it is done so genuinely and such that jam security. voting a ballot information is recorded on a blockchain, it is done so genuinely and such that jam security. Using an open blockchain to store and exchange trade e-voting ballot information creates genuine security issues: all data entered into the record is in clear, as is customary. Since each centre has an absolute copy of the record, the mystery of data can’t be ensured. The private blockchain is recommended to overcome the issues in the open blockchain. Private blockchain is a level above the converse of open blockchain. It is because various limits that are accessible to all on an open blockchain aren’t open here to all.

Figure 5.1: User Registration

## 5.4 Pre-Registration Of User

User registration is the necessary part of the electronic voting system since this system is web-based the registration has to be done earlier. According to the figure (Fig.3), the user must have to register with the virtual ID, which is obtained from the UIDAI, which is a temporary ID to get logged into the voting system. A VID is a regenerative number, i.e, valid for a minimum of one day or till the user re-generates it. VID is used for the authentication of the user and also for e-KnowYour-Customer services. Fig. 4: OTP service and authentication services by UIDAI. The CIDR (central identities data repository) is used by UIDAI to maintain Aadhar records and to Provide the user with the OTP for secure transactions, as shown in Fig. 4. Aadhaar Auth API [14]. Aadhaar validation is the procedure wherein an Aadhaar number, alongside different properties, is submitted online to the CIDR for its check based on data, information, or archives accessible with it.

## 5.5 Process of Voting

After the registration By verifying the details retrieved from the Aadhar database, the election commission officials decide whether the voter is eligible to cast a vote or not. Based on the decision of the election commission, a user has to cast their vote through the online voting web. Before the vote is submitted, the voter has to scan his/her QR code on a PC or mobile device. Then the vote is submitted and stored in the block in encrypted format using the private key. Asymmetric encryption is used for cryptographic operations

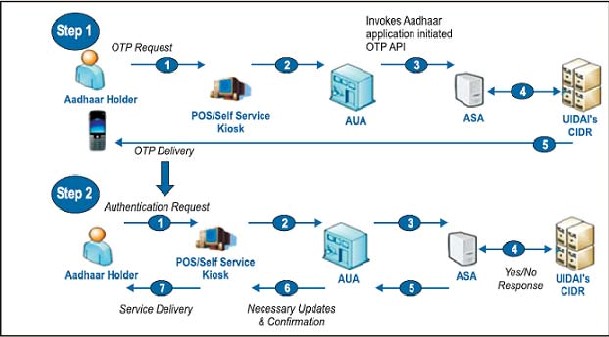


Figure 5.2: OTP service and authentication services by UIDAI.

like encryption and decryption, where the voter uses the election commission’s public key for the encryption process, and then the election commission members use their private key to decrypt and retrieve the vote to verify the votes. This framework has a strategy to execute activities on encoded information by utilising hash work with the assistance of a private key (VID), which can be recovered. By utilising public keys, election officials can de-encode information utilising square chain hash work calculation. On the other hand, all the voter details and the voting count will be updated to the election commission, but the data will be in the format of cipher-text and it should be decrypted for that election commission.

## 5.6 Hashing of Blocks in Blockchain

The blockchain is an appropriated record. It is partially open to everyone in the chain [11]. This blockchain has an intriguing property: when data is recorded inside a blockchain, it becomes difficult to change. Each square contains three segments.

1. Data,
2. The square hash

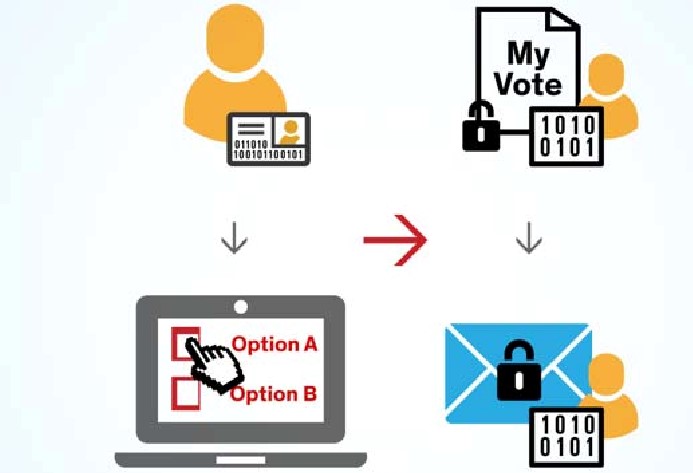
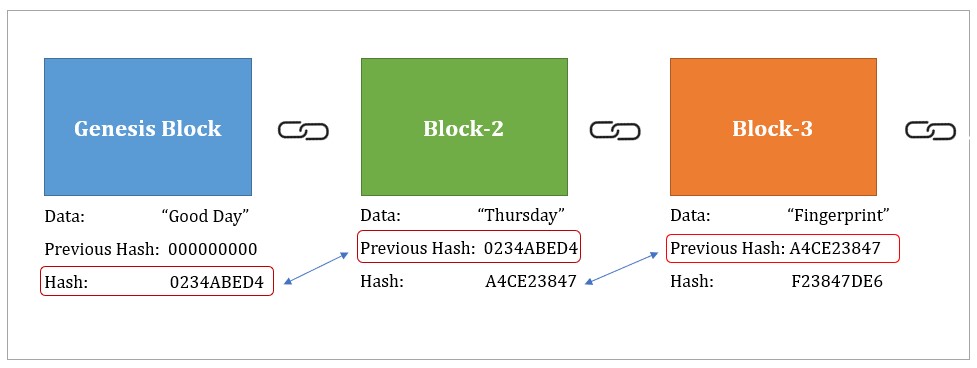


Figure 5.3: 3-Figure5-1 Figure 5.4: Hash Function

1. hash of the past square.

It includes the popularity of based data. It allows us to balance the hash. It is continually excellent. At the point when a square is made, its hash code has been resolved. If any changes are detected inside the square, it may make a hash code change. The hash is useful when you have to recognise changes to a square. As explained [11] in Fig. 8, initially once the voter casts their vote the new block will be created and using pairs of the keys, the hash is generated and continually the new blocks are created using the Hash of the previous block using some hashing algorithm. Hash can be generated using the private and public keys as shown in Fig. 9. This Hash ensures the integrity of the blocks which includes votes and voter information. SHA-256 is one of the hashing algorithms to ensure integrity, it provides the fixed length of 256bit of message hash output irrespective of the length of the input[12] [13].

## 5.7 Summary

Using an blockchain to store and exchange trade e-voting ballot information makes genuine security impediments: as is normally done, all data entered in the record is in clear. Since each center has an absolute copy of the record, mystery of data can’t be ensured.

To vanquish the issues in the open blockchain, the private blockchain is prescribed.

**Chapter 6**

# Blockchain Technology and Its Working

Over the past few years, you have probably heard the term ”blockchain technology,” probably regarding cryptocurrencies like Bitcoin. In fact, you may be asking yourself, ”What is blockchain technology?” It seems like blockchain is a platitude, but in a hypothetical sense, as there is no real meaning that the layman can easily understand. It is imperative to answer ”what is blockchain technology?” including the technology that is used, how it works, and how it’s becoming vital in the digital world. As blockchain continues to grow and become more user-friendly, the onus is on you to learn this evolving technology to prepare for the future. If you are new to blockchain, then this is the right platform to gain solid foundational knowledge. In this article, you will learn how to answer the question, ”What is blockchain technology?” You’ll also learn how blockchain works, why it’s important, and how you can use this field to advance your career.

## 6.1 Blockchain Technology

Blockchain technology is a structure that stores transactional records, also known as blocks, of the public in several databases, known as the ”chain,” in a network connected through peer-to-peer nodes. Hence, the information the digital ledger contains is highly secure. In simpler words, the digital ledger is like a Google spreadsheet shared among numerous computers in a network, in which the transactional records are stored based on actual purchases. The fascinating angle is that anybody can see the data, but they can’t corrupt it.

15

## 6.2 Popularity of Blockchain

Suppose you are transferring money to your family or friends from your bank account. You would log in to online banking and transfer the amount to the other person using their account number. When the transaction is done, your bank updates the transaction records. It seems simple enough, right? There is a potential issue which most of us neglect. These types of transactions can be tampered with very quickly. People who are familiar with this truth are often wary of using these types of transactions, hence the evolution of third-party payment applications in recent years. But this vulnerability is essentially why blockchain technology was created. Technologically, blockchain is a digital ledger that is gaining a lot of attention and traction recently. But why has it become so popular? Well, let’s dig into it to fathom the whole concept. Record keeping of data and transactions is a crucial part of the business. Often, this information is handled in-house or passed through a third party like brokers, bankers, or lawyers, adding time, cost, or both to the business. Fortunately, blockchain avoids this long process and facilitates the faster movement of the transaction, thereby saving both time and money. Most people assume blockchain and bitcoin can be used interchangeably, but in reality, that’s not the case. Blockchain is a technology capable of supporting various applications related to multiple industries like finance, supply chain, manufacturing, etc., but Bitcoin is a currency that relies on Blockchain technology to be secure. Blockchain is an emerging technology with many advantages in an increasingly digital world:

### 6.2.1 Highly Secure

It uses a OTP to conduct fraud-free transactions, making it impossible to corrupt or change the data of an individual by other users.

### 6.2.2 Decentralized System

Conventionally, you need the approval of regulatory authorities like a government or bank for transactions. However, with Blockchain, transactions are done with the mutual consensus of users, resulting in smoother, safer, and faster transactions.

### 6.2.3 Automation Capability

It is programmable and can generate systematic actions, events, and payments automatically when the criteria of the trigger are met.

## 6.3 Working of Blockchain

In recent years, you may have noticed many businesses around the world integrating blockchain technology. But how exactly does blockchain technology work? Is this a significant change or a simple addition? The advancements of Blockchain are still young and have the potential to be revolutionary in the future; so, let’s begin demystifying this technology. Blockchain is a hybrid of three key technologies:

1. Cryptographic keys
2. A peer-to-peer network containing a shared ledger
3. A means of computing, to store the transactions and records of the network.

Cryptography keys consist of two keys – a private key and a public key. These keys help in performing successful transactions between two parties. Each individual has these two keys, which they use to produce a secure digital identity reference. This secured identity is the most important aspect of Blockchain technology. In the world of cryptocurrency, this identity is used for authorising and controlling transactions. When they authorise a deal, it is certified by a mathematical verification, which results in a successful secured transaction between the two network-connected parties. So to sum it up, Blockchain users employ cryptography keys to perform different types of digital interactions over the peer-to-peer network.

## 6.4 Summary

Here we have learn how to master blockchain concepts, techniques, and tools like Hyperledger to build blockchain applications and networks.

**Chapter 7**

# Types of Blockchain

There are four different types of blockchains. They are as follows:

## 7.1 Private Blockchain Networks

Private blockchains operate on closed networks and tend to work well for private businesses and organizations. Companies can use private blockchains to customise their accessibility and authorization preferences, parameters for the network, and other important security options. Only one authority manages a private blockchain network.

## 7.2 Public Blockchain Networks

Bitcoin and other cryptocurrencies originated from public blockchains, which also played a role in popularising distributed ledger technology (DLT). Public blockchains also help to eliminate certain challenges and issues, such as security flaws and centralization. With DLT, data is distributed across a peer-to-peer network, rather than being stored in a single location. A consensus algorithm is used for verifying information authenticity; proof of stake (PoS) and proof of work (PoW) are two frequently used consensus methods.

## 7.3 Permissioned Blockchain Networks

Also sometimes known as hybrid blockchains, permissioned blockchain networks are private blockchains that allow special access for authorised individuals. Organizations typically set up these types of blockchains to get the best of both worlds, and it enables better structure when assigning who can participate in the network and in what transactions.

## 7.4 Consortium Blockchains

Similar to permissioned blockchains, consortium blockchains have both public and private components, except multiple organizations will manage a single consortium blockchain network. Although these types of blockchains can initially be more complex to set up, once they are running, they can offer better security. Additionally, consortium blockchains are optimal for collaboration with multiple organizations.

you will learn how to master blockchain concepts, techniques, and tools like Truffle, Hyperledger, and Ethereum to build blockchain applications and networks.

## 7.5 Summary

In this chapter we have learned types of Blockchain.Although these types of blockchains can initially be more complex to set up, once they are running, they can offer better security. Additionally, consortium blockchains are optimal for collaboration with multiple organizations.

**Chapter 8**

# Properties of Blockchain E-Voting System Using Vid

## 8.1 Authentication

This proposed system uses OTP to ensure security and also allows only registered voters to cast their votes, so that anyone can easily prove that the voter has cast their particular vote.

## 8.2 Availability

This proposed framework can be implemented anywhere across different countries based on their identities. Voters can check their voting eligibility at anytime.

## 8.3 Publicly Verifiable

Since the blockchain is one of the distributed and decentralised technologies, it makes other people in the election process able to verify the votes if they so intend and are authorized.

## 8.4 Integrity

The votes that are collected by the e-voting system should be accurate and tamperproof, and they should not be duplicated. Hashing helps in ensuring the integrity of the blockchain.

## 8.5 Sha Algorithm

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits. The other algorithms in the SHA family are more or less similar to SHA 256. Now, look into knowing a little more about their guidelines. It is a secure hash algorithm, which is under the family of cryptography where it helps with data security [12]. It works basically on hash functions. There are a few modules used in this; they are bitwise operators, modular adition, and comaparision functions.

## 8.6 Summary

In this chapter we learned that only registered voter can caste the vote. The voter can check their their eligibility to caste the vote.SHA alogorithm is used for the data security.

**Chapter 9**

# Testing

This chapter includes the details of Formal Technical Review meetings and describes the process carried during the review process. It also includes the Test Plan adopted for testing the

## 9.1 Formal Technical Review

Formal Technical Review (FTR) is a software quality control activity performed by software engineers.The purpose of FTR is to enable engineer to observe the analysis, design, coding and testing approach more closely. Formal Technical Reviews and Inspections of documents or software are performed to identify and remove defects.The Formal Technical Review of our project was carried at regular intervals The process included verification of the checklist which was developed for the review process, the code review checklist template is as follows:

## 9.2 Test Plan

Formal Technical Review (FTR) is a software quality control activity performed by software engineers.The purpose of FTR is to enable engineer to observer the analysis, design, coding and testing approach more closely.

|  |  |  |  |
| --- | --- | --- | --- |
| **Module being**  **Tested** | **Expected Result** | **Actual Result** | **Verdict** |
| Registration of user | User’s login detail will be gather successfully | User login detail gather successfully | PASS |
| Admin login | Admin login access created | Admin can new lo-  gin | PASS |
| Login via Password | User can access the voting pannel by using password | User was able to access login panel | PASS |
| Authentication via  OTP along with QR code Aadhar card as a base. | User will be allowed to cast vote if authentication succeeded else user will be prohibited. | If authentication successfully user will be allowed to vote if not then user is prohibited. | PASS |
| Generating  blockchain and adding a block to  it in firebase | New block is generated containing the data of user in firebase. | A new block gets generated and updated to the blockchain in the firebase. | PASS |
| Voting Casting and counting | Successfull votes are casted and counted | Successfully votes are getting cast and can see live  vote counting | PASS |

Table 9.1: Test Plan for E-voting based on Aadhar using blockchain technology

## 9.3 Publicly Verifiable

Since the blockchain is one of the distributed and decentralised technologies, it makes other people in the election process able to verify the votes if they so intend and are authorized.

## 9.4 Integrity

The votes that are collected by the e-voting system should be accurate and tamperproof, and they should not be duplicated. Hashing helps in ensuring the integrity of the blockchain.

## 9.5 Sha Algorithm

SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits. The other algorithms in the SHA family are more or less similar to SHA 256. Now, look into knowing a little more about their guidelines. It is a secure hash algorithm, which is under the family of cryptography where it helps with data security [12]. It works basically on hash functions. There are a few modules used in this; they are bitwise operators, modular adition, and comaparision functions.

## 9.6 Summary

In this chapter we learned that only registered voter can caste the vote. The voter can check their their eligibility to caste the vote.SHA alogorithm is used for the data security.

**Chapter 10**

# App Layout

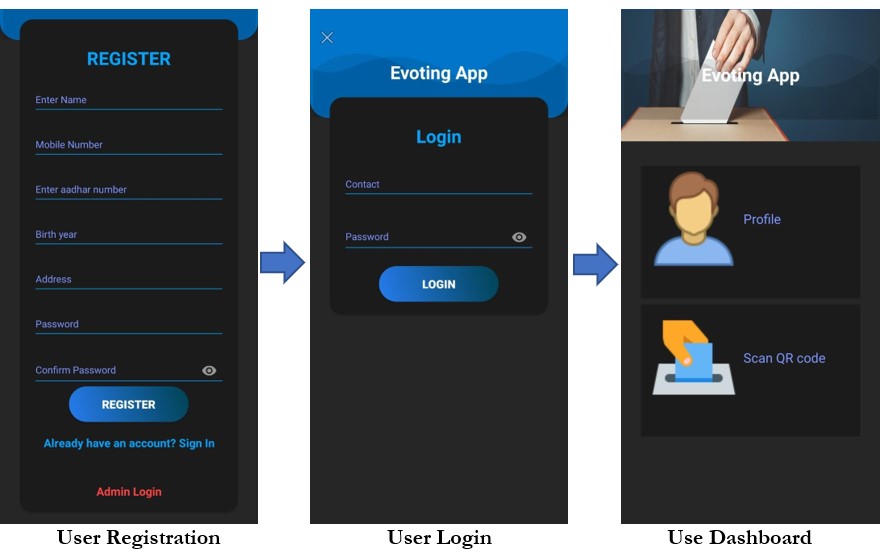


Figure 10.1: Registration-Login Interface

25

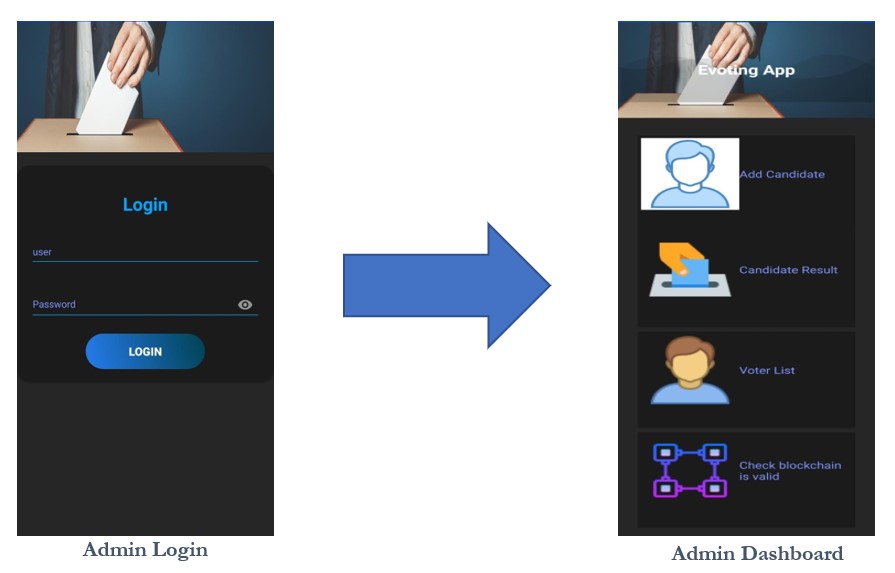


Figure 10.2: Admin Interface

**Chapter 11**

# Firebase Cloud

Firebase Cloud Messaging (FCM), formerly known as Google Cloud Messaging (GCM), is a cross-platform cloud solution for messages and notifications for Android, iOS, and web applications, which as of 2021 can be used at no cost.[1] Firebase Cloud Messaging allows third-party application developers to send notifications or messages from servers hosted by FCM to users of the platform or end users.

The service is provided by Firebase, a subsidiary of Google. On October 21, 2014, Firebase announced it had been acquired by Google for an undisclosed amount.[2] The official Google Cloud Messaging website points to Firebase Cloud Messaging (FCM) as the new version of GCM.[3] Firebase is a mobile platform which supports users in developing mobile and web applications. Firebase Cloud Messaging is one of many products which are part of the Firebase platform. On the platform users can integrate and combine different Firebase features in both web and mobile applications.

27

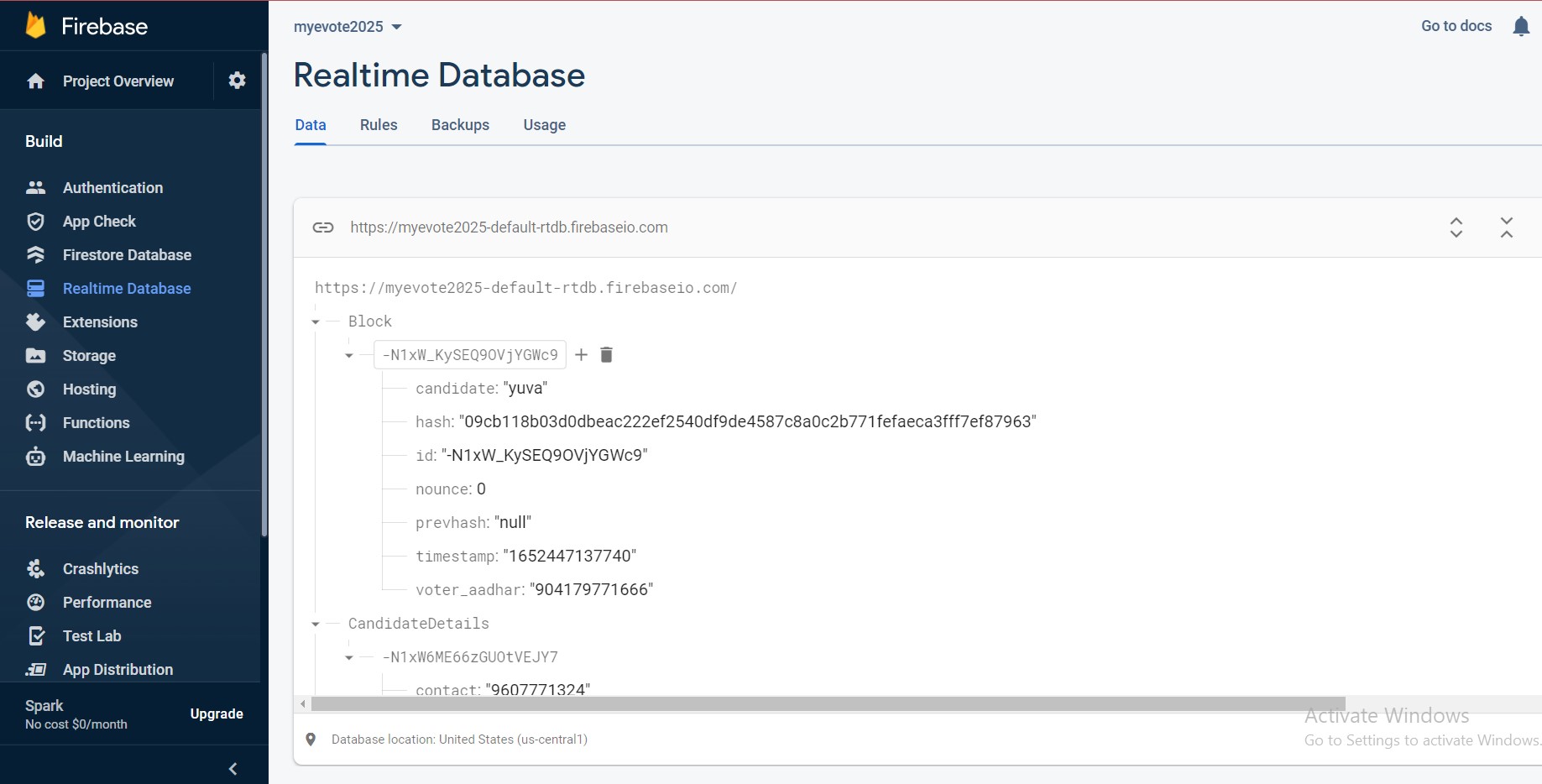


Figure 11.1: Real time database 1

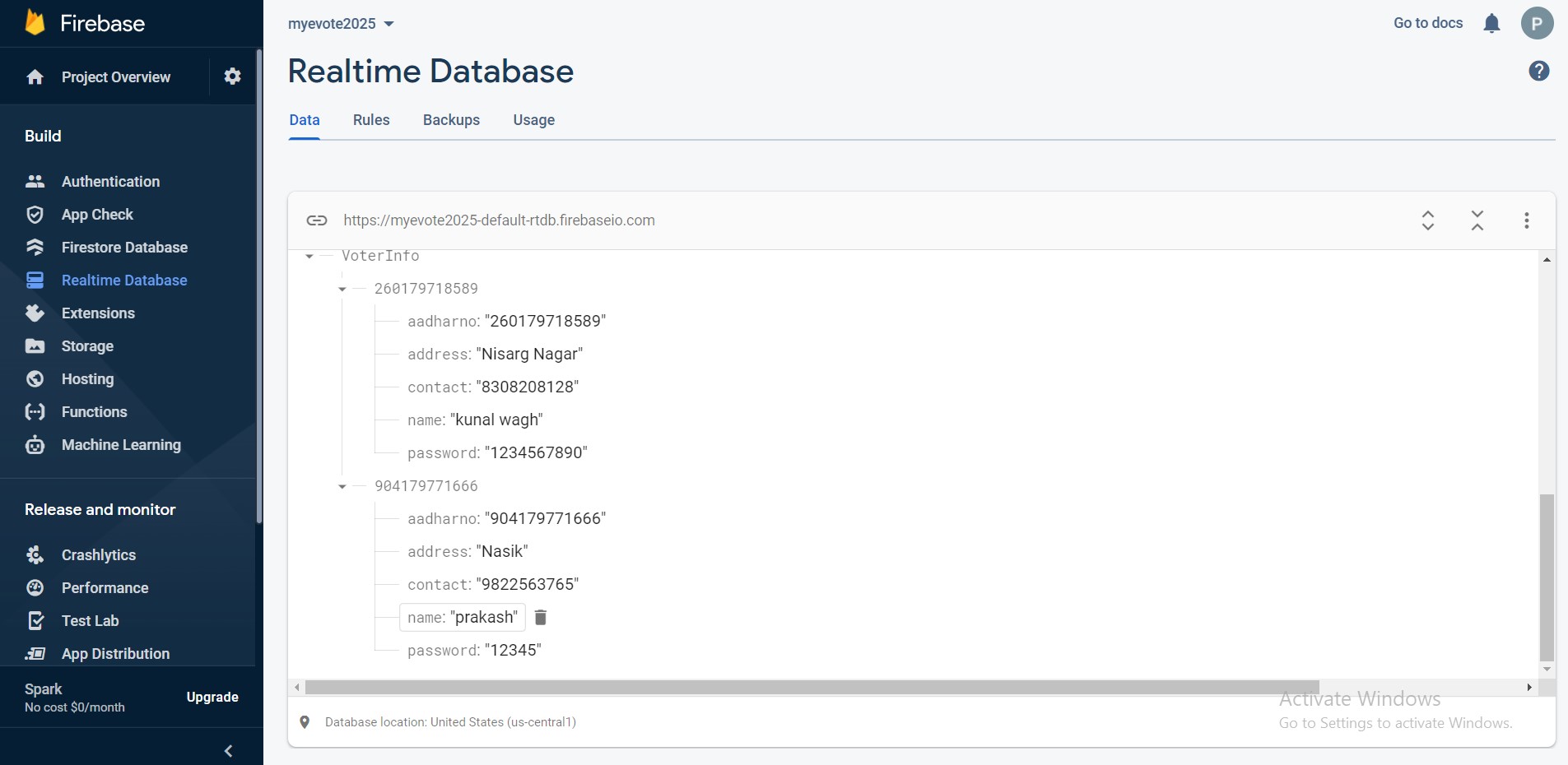


Figure 11.2: Real Time Database 2 E-Voting Based on Aadhar Using Blockchain Technology

## 11.1 Summary

Firebase cloud is used to store the information that we gather from users

MET’s Institute of Engineering 29

**Chapter 12**

# Conclusion

Voting is one of the processes which allows citizens to identify themselves in society. It is also one of the rights to choose a righteous and humble leader for society. There are many voting systems which are not secure, so the blockchain is used to ensure security by integrating the Aadhar verification using VID. OTP plays an important role here in ensuring security. Proceedings of the Second International Conference on Innovative Mechanisms for Industry Applications (ICIMIA 2020)

30

# Bibliography

1. *R*ifa Hanifatunnisa, et al, “ Blockchain Based EVoting Recording System Design”, School of Electrical Engineering and Informatics 2017.
2. *V* anessa Teague, Steve Schneider, Peter Y.A. Ryan, “End to End Verifiability in voting system from theory to practice” June2015.
3. *R*.Murali Prasad, et al, ”AADHAR based Electronic Voting Machine using Arduino”, International Journal of Computer Applications, vol. 145, no. 12, July 2016.
4. *D*esna Sebastian, et al, ”Aadhar Based ElectronicVoting System and Providing Authentication”, International Journal of Science and Engineering Research (IJ0SER), no. 3, March 2015.
5. *N*avya A et al, “Electronic voting machine based on Blockchain technology and Aadhar verification”. 2018 International Journal of Advance Research, Ideas and Innovations in Technology
6. *A*nsif Arooj and Mohsin Riazz “Electronic Voting With OTP Verification and Hybrid EVMs Solution” 2016.
7. *B*udi Rahardjo and Rifa Hanifatunnisa “Blockchain Based EVoting Recording System Design” 2017.
8. *h*ttps://hackernoon.com/how-blockchain-will-make-electronicvoting-more-securefba15d752bee.
9. *S*ivaganesan, D. (2019). Block Chain Enabled Internet of Things. Journal of Information Technology, 1(01), 1-8.

31

E-Voting Based on Aadhar Using Blockchain Technology

1. *D*evika K N, et al, “Parameterizable FPGA Implementation of SHA-256 using Blockchain Concept”. 2019 International Conference on Communication and Signal Processing.
2. *L*ukman Adewale Ajao, et al, “Crypto Hash Algorithm-Based Blockchain Technology for Managing Decentralized Ledger Database in Oil and Gas Industry” 2019.
3. *h*ttps://uidai.gov.in/images/FrontPageUpdates/aadhaar*authenticationapi*20*.pdf*

MET’s Institute of Engineering 32