

**ONLINE VOTING SYSTEM FOR INDIAN ELECTORAL  
PROCESS**

**(USING BLOCKCHAIN CONCEPT)**

A PROJECT REPORT

*Submitted in partial fulfilment of the requirements*

*for the award of the degree*

*Of*

**Computer Science and Engineering/Information Technology**

Under the supervision of

**Mr. Prateek Thakral**

(Assistant Professor)

*by*

**Bhawna(161476) and Sonali Sehgal(161235)**

**2016-2020**



**JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY**

**WAKNAGHAT, SOLAN – 173234**

**HIMACHAL PRADESH, INDIA**

# CERTIFICATE

## Candidate's Declaration

I hereby declare that the work presented in this report entitled “**ONLINE VOTING SYSTEM FOR INDIAN ELECTORAL PROCESS(USING BLOCKCHAIN CONCEPT)**” in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering/Information Technology** submitted in the department of Computer Science & Engineering and Information Technology, Jaypee University of Information Technology, Waknaghat is an authentic record of our own work carried out over a period from August 2019 to December 2019 under the supervision of (**Mr. Prateek Thakral**) (Assistant Professor, Computer Science and Engineering/Information Technology Department ). The matter embodied in the report has not been submitted for the award of any other degree or diploma.

Student

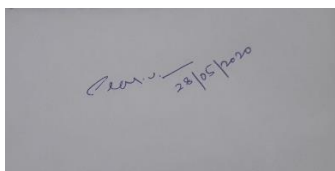
Bhawna(161476)



Sonali Sehgal(161235)



This is to certify that the above statement made by the candidate is true to the best of my knowledge.



(Supervisor Signature)

Supervisor Name: Mr. Prateek Thakral

Designation: Assistant Professor

Department name: Computer Science and Engineering/Information Technology

Dated: 28-05-2020

## **ACKNOWLEDGEMENT**

I would like to express my profound appreciation to all those who provided us the possibility to complete this report. A special gratitude we give to our final year project supervisor, Mr. Prateek Thakral, whose contribution in stimulating suggestions and encouragement, helped me and my partner to coordinate our project well especially in writing this report.

Furthermore, we would also like to acknowledge with much appreciation the crucial role of Jaypee University Of Information Technology, who gave the permission to use all the required equipment and the necessary materials to complete the project and framework of blockchain and solidify language. A special thanks goes to my supervisor, Mr. Prateek Thakral, who help me to assemble the parts and gave suggestion about the project” Digital Voting System using blockchain “. He has invested his full effort in guiding us for achieving the goal. We have to appreciate the guidance given by other supervisor as well as the panels especially in our project presentation that has improved our presentation skills thanks to the comments and advices.

Thanking You

Bhawna (161476)

Sonali Sehgal (161235)

## **ABSTRACT**

The building of an electronic voting system that satisfies the legal requirements of legislators has been a challenge for a long time. The increase in digital technology has revolutionized the life of people. Unlike the electoral system, there are many conventional uses of paper in its implementation. The aspect of security and transparency is a threat from widespread election with the conventional system(offline).

The general elections still use a centralized system, where in one organization manages everything. Some of the problems that can occur in traditional electoral systems is that with the organizations that has full control over the databases and the systems. It is possible to tamper with the database.

Blockchain technology is one of the solutions because it embraces a decentralized system and the entire database are owned by many users. Blockchain technologies offer an infinite range of applications benefiting from sharing economics. It is a disruptive technology that is playing a vital role in many sectors. It's revolutionary technology transforming the way we think about trust as it enables transacting data in a decentralized structure without the need to have trusted central authorities. Blockchain itself has been used in the Bitcoin system known as the decentralized Bank system. By adopting block chain in the distribution of databases on e-voting systems one can reduce the cheating sources of database manipulation. This project aims to implement voting result using blockchain algorithm from every place of election.

***Keywords:*** Security and Protection, Hardware, Online Information Services.

# **TABLE OF CONTENTS**

CERTIFICATE.....	
ACKNOWLEDGEMENT.....	
ABSTRACT.....	
ABBREVIATIONS .....	
LIST OF FIGURES.....	
<b>CHAPTER 1: INTRODUCTION</b>	
1.1 INTRODUCTION.....	
1.2 PROBLEM STATEMENT.....	
1.3 HOW THE VOTING TAKES PLACE ?.....	
1.4 PROJECT OBJECTIVES.....	
1.5 METHODOLOGY.....	
1.6 SOME BASIC TERMS USED IN PROJECT ABOUT BLOCKCHAIN.....	
1.7 ORGANIZATIONS.....	
<b>CHAPTER 2: LITERATURE REVIEW</b>	
2.1 BLOCKCHAIN BASED VOTING SYSTEM	
2.2 TOWARDS SECURE E-VOTING USING ETHEREUM BLOCKCHAIN	
2.3 BLOCKCHAIN VOTING AND ITS EFFECTS ON E-TRANSPERANCY	
2.4 A CONCEPTUAL SECURE BLOCKCHAIN BASED E-VOTING SYSTEM	
2.5 GENERAL WEBSITE AND RESEARCH PAPER SURVEYS	
<b>CHAPTER 3: SYSTEM DESIGNING</b>	
3.1 DESIGNING OF MODEL	
3.2 DATABASE VS BLOCKCHAIN	
3.3 STEPS TO BE FOLLOWED FOR MAKING BLOCKCHAIN VOTING SYSTEM	
3.4 ESSENTIAL REQUIREMENTS THAT NEED TO BE FULFILLED BY EVS IN	

NATIONAL ELECTIONS

3.5 EVALUATING BLOCKCHAIN AS A SERVICE FOR E-VOTING

**CHAPTER 4: DEVELOPMENT OF THE VOTING SYSTEM**

4.1 WRITING THE SMART CONTRACT USING SOLIDITY IDE REMIX

4.2 BUILDING THE APP INTERFACE

**CHAPTER 5: RESULT AND ANALYSIS**

5.1 DESCRIPTION

5.2 OUTPUT

5.3 SECURITY ANALYSIS AND LEGAL ISSUES

**CHAPTER 6: CONCLUSIONS**

**CHAPTER 7: PLAGARISM REPORT**

**REFERENCES**

## **ABBREVIATIONS**

P2P .....	Peer-to-Peer
PoS .....	Proof of Stake
RFID... ..	Radio Frequency Identification
RPC.....	Remote Procedure Call
BJP .....	Bhartiya Janta Party
EVS .....	Electoral Voting System

# **LIST OF FIGURES**

<b><u>Description</u></b>	<b><u>Page No</u></b>
<b>Fig. 1.1</b> Centralized Vs Decentralized Systems and Distributed Ledgers .....	
<b>Fig. 1.2</b> Client Server and P2P networks.....	
<b>Fig. 1.3</b> Blockchain Structure.....	
<b>Fig. 3.1</b> Database Architecture.....	
<b>Fig. 3.2</b> Blockchain Architecture.....	
<b>Fig. 3.4</b> E-Voting System ER Diagram.....	
<b>Fig. 4.1</b> Folder Structure.....	
<b>Fig. 4.2</b> Ganache Tool.....	
<b>Fig. 4.3</b> Adding Truffle Config file to create Workspace.....	
<b>Fig. 4.4,4.5</b> Output in the terminal during deploying of contracts.....	
<b>Fig 4.6</b> Adding Localhost network to the Metamask extension.....	
<b>Fig 4.7</b> Capturing Private Key from Accounts Tab in Ganache Tool.....	
<b>Fig 4.8</b> Passing private key string over the MetaMask for connectivity.....	
<b>Fig 4.9</b> Executing React application through this command.....	
<b>Fig 4.10</b> Main Page of Digivote after execution.....	
<b>Fig 5.1</b> Organizer Login Page.....	
<b>Fig 5.2</b> Organizer Registration Page.....	
<b>Fig 5.3</b> Candidate Login Page.....	
<b>Fig 5.4</b> Candidate Registration Page.....	
<b>Fig 5.5</b> Election Registration Page.....	
<b>Fig 5.6</b> Candidate Dashboard.....	
<b>Fig 5.7</b> Candidate Request.....	



**Fig 5.8** Organization Approval Dashboard.....

**Fig 5.9** Live Elections.....

**Fig 5.10** Vote candidates.....

**Fig 5.11** Aadhaar Card Verification.....

**Fig 5.12** Voter Card Verification.....

**Fig 5.13** Lok Sabha Vote for Candidate.....

## **TABLES**

### **Description**

### **Page No.**

**Table 3.1.** Database Vs Blockchain (Permission and Private) .....

# **CHAPTER-1**

## **INTRODUCTION**

### **1.1.Introduction**

The Election Commission of India is an autonomous constitutional authority responsible for the conduct of Union and State election procedures in India.

The body elections are held in India for the Lok Sabha, the Rajya Sabha, the state assemblies and the offices of the President and Vice President in the country.

India, being a union of states, has separate state assemblies for each state. The state assemblies have a governor and two houses - the Legislative Council and the Legislative Assembly.

#### **1.1.1. Social advantages of the system:**

- The program increases the number of voters who experience difficulty in voting.
- It is a quick and safe way to vote and increases the number of voters as the process does not take much of their time.
- While the plan is very transparent and can be followed, it helps to build trust between the people in government.
- Voting The blockchain voting system is environmentally friendly as compared to the paper voting system. It eliminates the need for paper ballots and reduces the carbon emissions from the materials of those votes. Therefore, the system has a low carbon footprint.
- Here by, Elections are an important part of a democracy. Any management team or oversight council will fulfill their responsibility honestly in relation to changing the way decisions are made. The blockchain distributes the voting framework that governs voter protection and assessment and provides a direct and accessible framework for assessing voting companies. Alternatively, the blockchain class is not cost effective compared to the standard framework and may change the voting method.

## **1.2. Problem Statement**

Electoral process is very important event in modern democracy. The issue with the present polling form framework is that it tends to be handily controlled by power hungry associations. A need emerges to take out the part of trust from a political decision to make it secure and straightforward. Also, many people are not able to vote because of their absence in respective hometown at the time of event.

- A system is required to make easier and quicker voting process. Election system needs to be more accessible to all voters leading to higher voter turnout.
- We propose to overcome these problems by removing voters' location bar and minimizing third party involvement for securing the data.

## **1.3. How Does Voting Take Place?**

Voting is done by secret ballot.

- Polling Stations are normally set up in open establishments, for example, schools and network corridors.
- The Election Commission puts forth all attempts to guarantee that a voter need not travel multiple kms. to arrive at the surveying station.
- Efforts are likewise made to save the quantity of balloters for each surveying station inside 1200.
- Each surveying station is open for at any rate 8 hours upon the arrival of the political race.
- On entering the surveying station, the balloter is checked against the Electoral Roll and personality report is confirmed, permanent ink is applied on the left index finger and a voter slip is given and the voter is permitted to make their choice by actuating the polling form button in the control unit by the managing official.

## **1.4. Project Objectives**

The online voting system provides a voting service that allows people to vote from anywhere in the country electronically. This system is designed to improve the current voting process in the following ways:

1. We have to Allow voters to vote from any poll site in the country.
2. We have to Reduce the number of legitimate votes by eliminating vote tampering
3. We have to Improve the registration process by allowing voters to check their registration status prior to voting and centralizing registration databases.
4. We have to Increase voter confidence and improve the voting experience.

This all can be done using Blockchain concept.

## **1.5. Methodology**

*Voting System Basic App structure using Blockchain-*

### **1.5.1. What will this app do?**

It will display some specific voting choices. It will allow users to vote for 1 of the choice. It will allow the administrator to end the polling and display the results.

### **1.5.2. How will we do it?**

1. We will write a smart contract.
2. We will build the interface.
3. We will install testrpc.
4. We will connect smart contract and interface.
5. We will run the app locally using testrpc and web3.

### **1.5.3 Technology Used-**

1. Ethereum Blockchain
2. ReactJS
3. Web3JS
4. IPFS : for decentralize data storage.

## **1.6. Some Basic Terms Used in the Project About Blockchain:**

### **1.6.1. What is blockchain?**

Blockchain is digital ledger, i.e. growing list of records that keeps track of transactions.

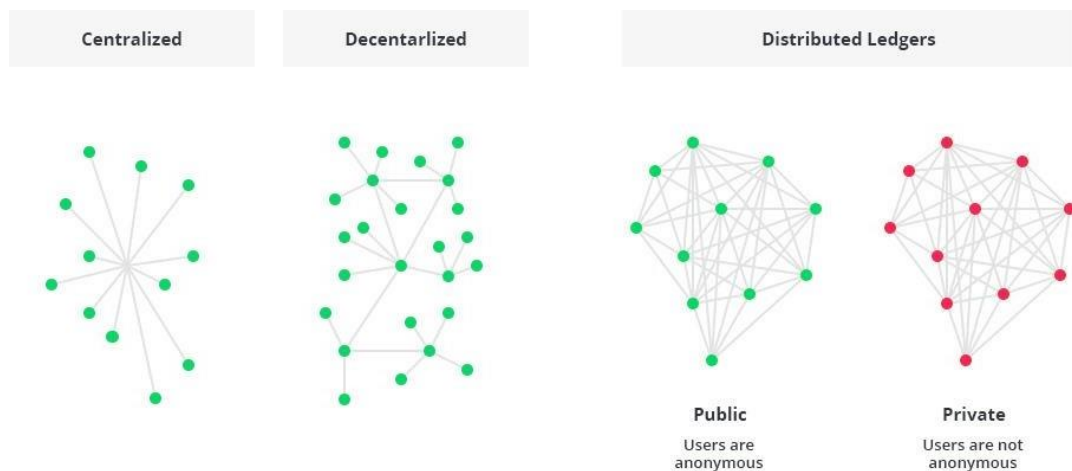
Transactions can be anything from money transfers to blog posts to votes. Transactions are compiled into blocks and added to the end of the current chain. Blockchain is structured in the form of linked list where blocks are nodes.

Blockchain is unique as it is a decentralized system. It is maintained by peer to peer network rather than being maintained and controlled by one single entity. Due to linked like structure, it is impossible to modify existing transactions. Blockchain is an open platform which makes transactions easy to verify.

### 1.6.2. Advantages of blockchain:

6. Increased security through cryptography and hashing algorithms.
7. It is almost impossible to tamper with previous transactions.
8. It is seamless and instantly updates across the entire blockchain network.
9. There is no point of failure.
10. It is easy to verify and see previous and present transactions.

### 1.6.3. Centralization and decentralized system difference:



*Fig.1.1. Centralized VS Decentralized Systems and Distributed Ledgers*

**Centralization** is the convergence of control of a movement or association under a solitary position. This implies in brought together stage there's a solitary purpose of contact for example a private center point.

**Decentralized** is the development of divisions of a huge association away from a solitary managerial focus to different areas. This implies there is no single purpose of contact all work all alone and the manner in which they need for example (P2P) arrange.

The greatest contrast between the two Blockchains is of the pool of the hubs that may participate in the system and may partake in the system and may make changes as an administrator to the system. To comprehend, there is a case of Bitcoin the biggest open Blockchain that has no limitation with regards to getting to the record and sharing PC capacity to play out its confirmation of work calculation. While, IBM's Hyperledger Fabric Blockchain is progressively adjustable the association that is utilizing it has command over every viewpoint and can take dynamic interest in the Blockchain. This implies private Blockchains are prohibitive as far as making changes as Blockchain is utilized for inward records and just the individuals who have the consent can make modifications to private Blockchains.

There is a distinction of Ownership among Centralized and Decentralized trades. In the event of Centralized trades, they work also to banks and trades today. There is a proprietor. There is a safe. There are rules and guidelines. In spite of the fact that this incorporated model has existed for quite a long time, the possibility of a decentralized trade is new. The idea is just conceivable with the making of crypto resources and a straightforward, unchanging record. Utilizing the blockchain to monitor proprietorship without an outsider, we can make a commercial center for trading these advantages that work without consent or oversight.

A decentralized stage relies upon the host of PCs because of which Blockchain innovation takes a shot at a P2P organize. While the unified stage is a private and they don't require as much force as required by decentralized Blockchain.

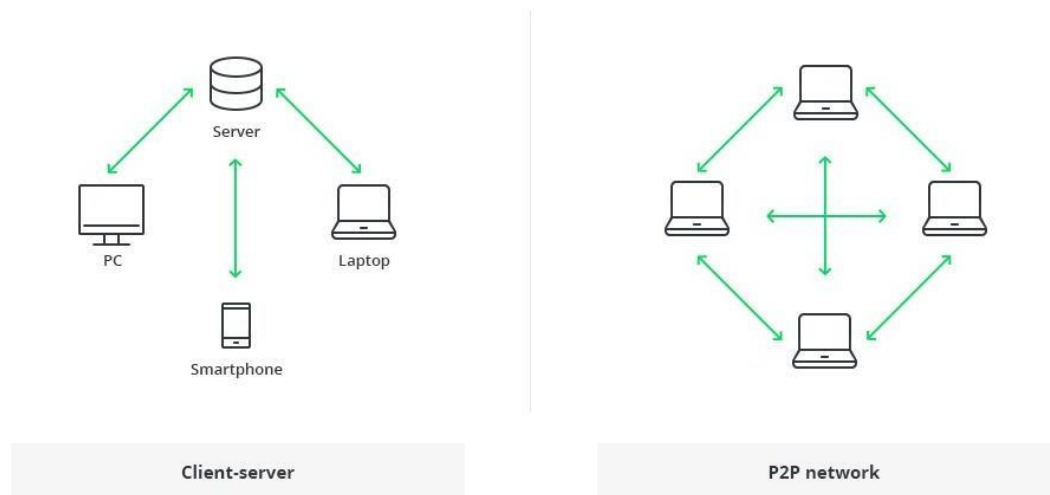
#### **1.6.4. Disseminated records (open versus private blockchain)**

Both the two kinds of blockchains, Public and private, are decentralized, distributed systems. Each individual from the chain keeps up an imitation of a common record that stores carefully marked record that stores carefully marked exchanges. This record must be annexed to, yet not altered. Members in a blockchain keep this record in a state of harmony through an accord convention. This makes an assurance on the permanence of the record which can't be adulterated regardless of whether there are some noxious members on the blockchain. The distinction among open and private blockchain is identified with the kind of members permitted inside the system that keep up the record and executes the agreement convention.

Open blockchains are open systems that permit anybody to partake in the system, subsequently the name 'open'. Such a system relies on the quantity of members for its prosperity. Consequently, they support increasingly more open interest through a boost instrument. The best model is Bitcoin.

In Private Enterprises can set up private blockchains to ensure the protection and security of their information. Cooperation in a private blockchain requires a greeting, which itself is additionally approved by the system starter or a lot of decides that can establish. Such a system is known as a permissioned system, and puts a limitation on who is permitted to join. Private blockchains can likewise limit members movement with the end goal that specific exchanges must be completed by specific members and not others, in spite of the way that they are on the system.

#### **1.6.5. Client server and P2P networks**



*Fig. 1.2. Client Server and P2P networks*

The customary engineering of the World Wide Web utilizes a customer server arrange. For this situation, the server keeps all the necessary data in a single spot so it is anything but difficult to refresh, because of the server being an incorporated database constrained by various overseers with consents.

On account of the conveyed system of blockchain design, every member inside the system looks after, affirms, and refreshes new passages. The framework is controlled by isolated people, yet by everybody inside the blockchain arrange. Every part guarantees that all records and systems are all together, which brings about information legitimacy and security. In this manner, parties that don't really believe each other can arrive at a typical accord.

#### **1.6.6. What is decentralization?**

It is a system that is governed by lots of smaller parties rather than one single entity. Decentralization in blockchain means that the entire blockchain is managed by everyone using it rather than one company. This means that everyone shares equal control over everything that happens.

#### **1.6.7. Advantages of decentralization:**

1. There is no single point of failure as network is everyone.



2. Transactions are easy to verify as everyone has equal say and can see the transaction history.
3. There are instant updates across the entire platform.

### 1.6.8. Who governs a blockchain?

Blockchain is governed not only by single person or group but by everyone. Everyone has equal say over what is approved or not in a blockchain.

Miners, the people who group transactions and build blocks, build and maintain the blockchain's structure.

### 1.6.9. How are blockchains structured?

A blockchain is a linked list or a chain of blocks. Blocks contain all the transaction data and typically contain multiple transactions. Blocks are added to the end of the chain during the mining process. Mining compiles several transactions with info about them into a block and adds them to the end of the blockchain, thus executing them.

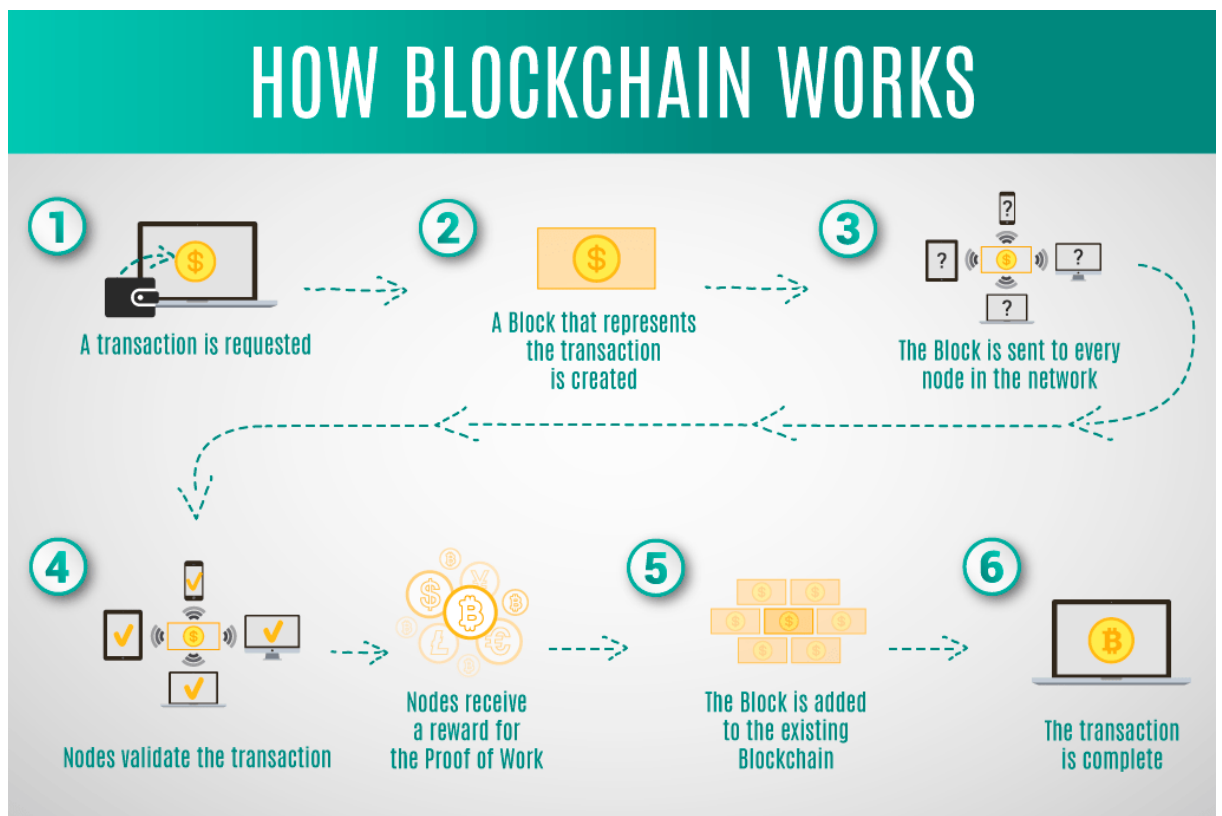


Fig.1.3. Blockchain Structure

#### **1.6.10. What is Ethereum blockchain?**

It is just another blockchain that is a digital ledger used to store a list of transactions.

Mining generates Ether. It is designed with decentralized apps in mind.

#### **1.6.11. Ethereum vs. bitcoin blockchain**

**Ether** is a cryptocurrency in which coins per block are consistent and transaction fees vary based on amount of computation required. It is the fastest transaction method i.e. takes 10 to 20 seconds. Ethereum uses ether to run decentralized apps.

**Bitcoin** is a cryptocurrency in which coins per block halves every 4 years and transaction fees are consistent. It has slow transaction time i.e. 10 minutes. Its focus is on crypto currency.

#### **1.6.12. What makes Ethereum good for decentralized apps?**

Consistent coins per block means there is no decrease in incentive to keep mining. Transaction fees is based on computation means that some transactions are cheap to execute if contracts are written well. Also, relatively fast transactions prevent frustration.

#### **What is a decentralized app?**

It is the Web app that runs on a decentralized system, in our case it a blockchain. It is different from regular web apps that are stored on a server somewhere and run on the server. Decentralized apps run like regular apps but rather that storing data in a server, they store data and transactions on the blockchain.

In Decentralized apps server fees is replaced by transaction fees (on the Ethereum blockchain, this is called Gas). The transactions are not hidden or censored. Data on a blockchain only exists on the blockchain so it must receive outsider data elsewhere. This outsider data is provided by Oracles to the blockchain from external sources. Data is made available through API calls. Oracles are tested and trusted sources and the entire blockchain takes data from several sources before coming to a final consensus.

#### **1.6.13. How do D-Apps Run?**

Outwardly, Decentralized apps run like any other web apps. But inwardly, data is fetched/ added on a blockchain instead of a server. Data fetch calls retrieve previous transactions

from a blockchain. Data adding/ modifying calls add new transactions to a pool of transactions to process to add new data or provide new values for existing data.

#### **1.6.14. How is Data Fetched, Added, or Modified in a D-App?**

Smart Contracts are like files that dictate how data should be used within a D-App; sometimes, this involves executing one or more transactions. Transactions are only executed once selected, compiled into a block, and the block is successfully mined. There is a cost associated with writing (but not reading) to the blockchain.

#### **1.6.15. What is a Smart Contract?**

It is a protocol that ensures both parties honour an agreement and the correct actions will take place. Correct actions could be casting a vote, placing a bid, transferring funds, or even posting a new blog post. It means that a transaction or set of transactions will be executed properly every time.

#### **1.6.16. How are smart contracts secure?**

The programmer who writes a smart contract makes sure to cover every possible case and to ensure that correct actions take place, whether it's executing a transaction, triggering an exception, or refunding gas. Once transaction is executed, it cannot be reversed due to the nature of a blockchain. This ensures security and eliminates the need for a moderator to make sure that both parties honour the agreement.

#### **1.6.17. How are smart contracts written?**

Most Ethereum smart contracts are written in Solidity. Contracts are very similar to classes in Object Oriented languages. It has Constructors to start new instances, fields to store data and Methods to execute behaviours. Any functionality to retrieve or read values costs nothing. Functionality to create or update variables or perform an action costs amount of gas.

### **1.7. Organization**

Secure and transparent digital voting system is made by us for use by the country to conduct Elections. We leverage the unique attributes of blockchain technology to design the next generation of voting system for governments and organizations.

## **CHAPTER-2**

### **LITERATURE SURVEY**

#### **2.1 Blockchain-Based E-Voting System**

##### Summary:

This paper [1] assesses the utilization of blockchain as a help to actualize an electronic democratic (e-casting a ballot) framework. The paper makes the accompanying unique commitments: (I) inquire about existing blockchain structures appropriate for developing blockchain based e-casting a ballot framework, (ii) propose a blockchain-based e-casting a ballot framework that utilizes "permissioned blockchain" to empower fluid majority rules system. The token of this paper is sorted out as follows: Section II talks about structure contemplations for political race frameworks. Area III shows our blockchain based e-casting a ballot framework and assess a portion of the mainstream blockchain structures for understanding the framework. Segment IV talks about a portion of the security and lawful contemplations and restrictions in regards to planning an electronic democratic framework for national races. Related work is exhibited in Section V and ends in area VI.

#### **2.2 Towards Secure E-Voting Using Ethereum Blockchain**

##### Summary:

In this work [2], association has executed and tried an example e-casting a ballot application as a shrewd agreement for the Ethereum organization utilizing the Ethereum wallets and the Solidity language. Android stage is additionally considered to permit deciding in favour of individuals who don't have an Ethereum wallet. After a political race is held, in the end, the Ethereum blockchain will hold the records of voting forms and votes. Clients can present their votes by means of an Android gadget or legitimately from their Ethereum wallets, and these exchange demands are taken care of with the agreement of each and every Ethereum hub. This agreement makes a straightforward domain for e-casting a ballot. Notwithstanding an expansive discourse about unwavering quality and productivity of the blockchain-based e-casting a ballot framework, the application and its test outcomes are likewise exhibited in this paper.

### **2.3 Blockchain Voting and Its Effects on Election Transparency**

#### Summary:

In this research [3], ACM investigate the plausibility of utilizing Blockchain innovation to help in tackling those straightforwardness and certainty issues. To start with, the paper gives an outline of Blockchain itself and different uses concentrated on cultural issues and their particular examination. At that point, breaks down how the reception of Blockchain into an advanced government collection can add to regular e-casting a ballot issues and furthermore advance races straightforwardness, increment auditability, upgrade voter certainty and fortify majority rules system. Assists working with clearing comprehension of what is Blockchain and its fundamental ideas, why are market and specialists so amped up for it, how it can unravel normal democratic frameworks issues, who is as of now utilizing it and the advantages and potential dangers of its selection.

### **2.4 A Conceptual Secure Blockchainbased Electronic Voting System**

#### Summary:

This paper [4]assesses prior proposed electronic democratic framework models. The main ever electronic democratic framework was presented in the mid-eighties by David Shaum. The framework utilized an open key cryptography, which was utilized to cast votes and keep voters unknown. To ensure there were no connections among voters and voting forms, the Blind Signature Theorem was utilized. Estonian I-Voting System model elaboration; Estonia was the primary nation where residents had the option to make their choice utilizing just the Internet and an electronic national distinguishing proof card. The ID card utilized in the decisions was intended to run on a coordinated circuit, a chip Java chip stage, and secured with 2048-piece PIN. Additionally, this paper presents model to use the open source Blockchain innovation to propose a plan for another electronic democratic framework that could be utilized in nearby or national races.

### **2.5 General Website and Research Paper Surveys:**

[5]Progressively computerized innovation in the present helped numerous individuals lives. In contrast to the constituent framework, there are numerous customary employments of paper in its usage. The part of security and straightforwardness is a risk

from still far reaching political decision with the ordinary system(offline). Blockchain innovation is one of arrangements, since it grasps decentralized framework and the whole database are possessed by numerous users.[1]

Bit coin presents a progressive decentralized agreement component. In any case, Bit coin-determined accord components applied to open square chain are insufficient for the organization situations of growing consortium square chain. We propose another agreement calculation, Proof of Vote (POV). The previous ensures the detachment of casting a ballot right and official right, which improve the freedom of bulter's job, so does the inward control framework inside the consortium. Concerning the last mentioned, under the situation that in any event  $Nc/2+1$  magistrates working adequately, our investigation shows that POV can ensure the security, exchange?

There is no uncertainty that the progressive idea of the blockchain, which is the fundamental innovation behind the celebrated cryptographic money Bitcoin and its successors, is setting off the beginning of another period in the Internet and the online administrations. In this work, we have executed and tried an example e-casting a ballot application as a savvy contract for the Ethereum organize utilizing the Ethereum wallets and the Solidity language.

Square chain was first presented by Satoshi Nakamoto (a pen name) who proposed a distributed instalment framework that permits money exchanges through the Internet without depending on trust or the requirement for a monetary establishment. Square chain is secure by structure, and a case of a framework with a high byzantine disappointment resistance.

Evidence of stake convention of square confirmation doesn't depend on over the top calculations. It has been actualized for Ethereum and certain altcoins. Rather than parting hinders crosswise over relatively to the relative hash paces of excavators (for example their mining influence), evidence of-stake conventions split stake squares relatively to the present abundance of excavators. The thought behind Proof of Stake is that it might be increasingly hard for diggers to procure adequately huge measure of computerized money than to secure adequately amazing registering hardware

## **CHAPTER 3**

### **SYSTEM DEVELOPMENT**

#### **3.1 Designing of model**

Usually when interacting with a web application, you use the web application to communicate with the central server at the top of the framework. All code for this web application resides on this central server, and all data resides on the central database. In any event you make your request, you should talk to this central server on the web.

If we could somehow compile our democratic system on the web, we could run into a few problems:

1. The information in the database can be changed: it can be checked often, or extracted.
2. The source code on the web server can also be changed at any time.

We prefer not to develop our app on the web. We have to build it on a blockchain where anyone related to the framework can look into political competition. We must ensure that their votes are tested, and that they are counted only once. So, we have to research how that works.

As opposed to having a framework, a centralized server and a database, blockchain is custom and database no matter how you look at it. The blockchain is a shared arrangement of PCs, called center points, that provide all the information and code in the framework. So, on the off chance that you are a blockchain-related tool, you are at the center of the framework, and are talking about different PC points in the framework. You also have a copy of the comprehensive database and code on the blockchain. There are no intermediate servers in progress. Just a ton of PCs talking to each other through a comparison framework.

Instead of aggregated data, all of the exchange information that is shared over blockchain locations is contained in groups of records called squares, which are grouped together to form an open record. This open record addresses all information on the blockchain. All information in the open code is verified by cryptographic hashing, and is allowed for calculation of the agreement. Hubs in the system take the interest of

making sure all duplicates of information shared over the system are equal. This is one important reason why we collect our democratic system in blocks, considering that we need to ensure that our vote is tested and consistent.

### 3.2 Database vs Blockchain

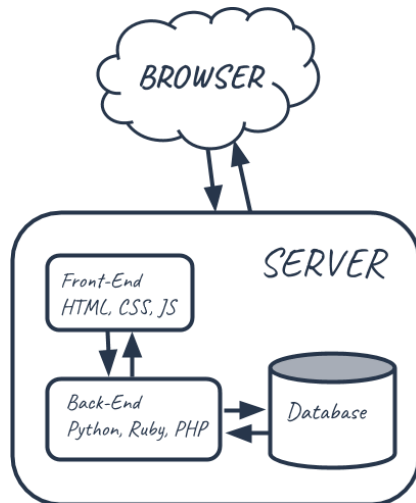


Fig. 3.1. Database Architecture

A database depends on customer/server engineering. It is an exceptionally effective architecture that can take a shot at both little scale and enormous scale conditions. Here the customer is beneficial while the servers go about as a brought together handling unit. The correspondence among customer and servers are kept up through a safe association.

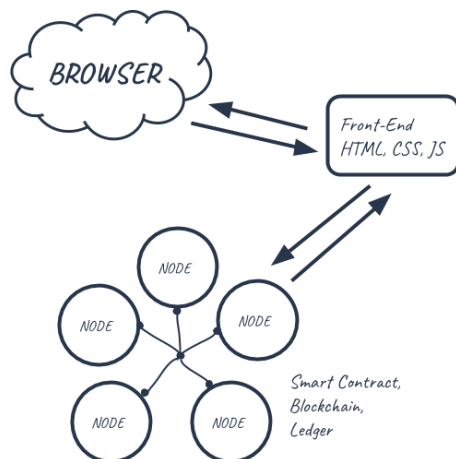


Fig. 3.2. Blockchain Architecture

Blockchain utilizes a conveyed record arrange engineering. It is a distributed empowered system where each friend can interface with another utilizing secure cryptographic



conventions. As there is no brought together hub, hubs can by and large partake in the agreement calculation. One of the most famous calculations is Proof of work which expects diggers to explain complex scientific conditions to approve exchanges over the system.

### **Blockchain vs. Centralized Database: Authority and Control**

In the event that we look at the blockchain and the database, the main thing you will see is the means by which authorization works. The intention of the blockchain is to work in a decentralized manner while databases are constantly brought together. This remarkable component of blockchain gives it the impact it needs to transform innovation in the up and coming era.

Decentralization achieves a great deal of usage changes in current frameworks and processes used by various undertakings. This enables the system to work independently and to evacuate any requirement for integrated control.

The database, then, depends entirely on the corporate perspective. No customary database fills with decentralization. In the event that you are explicitly looking for a decentralized database, at that point the blockchain legitimately falls into the class.

How about we check how centralization works in the database. An overseer is assigned to deal with the database. The director has all authority over the database, which means that he can maintain, change and control the database in the manner in which it is needed. Without the chairman, the database would not work by any stretch of the imagination. He is on top and can do a lot without creating, changing, changing and erasing records. In addition, they can similarly perform various undertakings, for example, execution advancement. It is an important undertaking as a large undertaking which will normally be delayed after some time.

With respect to different clients related to the database, an administrator can assign jobs to different clients. Different clients can work with the database they are assigned to. For example, he can deli a client to create new clients. Other key capabilities, for example, database support, maintenance, and so on, should also be possible.

In any case, it is not basic, when we think of different types of blockchain. The basic blockchain introduced in bitcoin is completely decentralized, anyway it cannot be realized among organizations that have private data and methodology. The same explanation is made blockchain, and we have an alternative type of blockchain. Crossbreed / Federated blockchain is the most notable type of blockchain that deals with the issue of personal affiliation.

Hybrid blockchain is allowed that gives affiliation the full ability to change its course of action as needed.

When we do database versus private blockchain, this is the best possibility. We will cover logically about mutual / private blockchains later in the article.

### **Blockchain Database vs. Traditional Database: Architecture**

Architecturally both blockchain and database are extraordinary. Things being what they are, what is the contrast between blockchain database structure and conventional database structure?

A database depends on customer/server engineering. It is a profoundly fruitful engineering that can take a shot at both little scale and huge scale conditions. Here the customer is beneficiaries while the servers go about as a brought together preparing unit. The correspondence among customer and servers are kept up through a safe association.

Blockchain, then again, utilizes a conveyed record arrange engineering. It is a shared empowered system where each companion can associate with another utilizing secure cryptographic conventions. As there is no brought together hub, hubs can all things considered participate in the agreement calculation. One of the most prevalent accord calculations is Proof-of-Work which expects diggers to settle complex scientific conditions to approve exchanges over the system.

The database does not require an agreement calculation and is subject to a completely simultaneous approach. The chairman controls each part of the database and is exceptionally involved. Likewise half-breed is allowed like a blockchain, yet not unlike with the open blockchain. It ideally responds to your probes identified with the allowed blockchain vs. database. Also the table allowed blockchain vs. database.

	Database	Hybrid/Federated Blockchain	Public Blockchain
Type	Permissioned	Permissioned	Public
Control	Centralized	Hybrid with few features centralized	Decentralized
Architecture	Client-Server architecture	Closed architecture	Peer-to-Peer Public peer-to-peer architecture
Data persistence	non-persistence	Immutable	Immutable
Chance of failure	Yes	No	No
Performance	Extremely fast	Slow to medium	Slow

*Table 3.1. Database vs. blockchain (permissioned and private)*

### **Blockchain vs. Database: Immutability and data handling**

With regards to information stockpiling and taking care of, both blockchain and database work in an unexpected way. In a customary database, information can be put away and recovered easily. To guarantee legitimate activity of the application, CRUD is used at the essential level. Muck represents Create, Read, Update and Delete. This additionally implies information can be eradicated and supplanted with new qualities if necessary.

Blockchain, then again, works diversely with regards to information stockpiling. Blockchain underpins permanence which implies that information once is composed can't be eradicated or supplanted. Unchanging nature implies that no information altering is conceivable inside the system. Conventional databases don't show unchanging nature and subsequently are progressively inclined to being controlled by a rebel director or outsider hacks.

In short, Blockchain only supports two operations, Read and Write.

- Read Operations: Used to read or retrieve data from the blockchain network
- Write Operations: Used to add information and data to the blockchain network

## **Blockchain vs. Database: Transparency**

Another key property that blockchain offers is the means by which anybody with the correct apparatus can confirm the information once composed into the open blockchain. Straightforwardness guarantees that people in general can confide in the system.

Databases, then again, being unified, doesn't bolster any type of straightforwardness. Clients can't check the data on the off chance that they need to. Be that as it may, a head can make a lot of information open, yet at the same time, the information confirmation is impossible by a person.

Blockchain's respectability is made conceivable gratitude to the unchanging nature it brings to the table. Information once put away can't be undermined or changed in any conceivable manner, which implies that the information uprightness is kept up at any expense.

## **Blockchain vs. Database: Cost and Talent Acquisition**

A customary database is less expensive when contrasted with blockchain, in relation to usage costs. Blockchain is indeed a new innovation and therefore evolving yet. Similarly a business means that the blockchain needs to make proper arrangements and execution to coordinate its process. Additionally, any business that is now operating needs to receive new innovation. Adjustment to the approach is a real business as the blockchain is expected to end execution and simply cannot be included in the current framework as an addition.

Traditional databases are anything but difficult to set up and scale. They work with a large part of the current processes and later work out of the crate in several frameworks. This is a wonderful decision for a business that needs to rapidly and cost-successfully set up its database framework.

In any case, on the off chance that we take a lump at the expense associated with every innovation for a more attracted person, blockchain can provide more arrangement as friends for the most part deal with the system . Associations are not required to manage additional expenses related to working with the system, which can save a ton of expense.

Equivalent cannot be said in relation to attaining capacity. Blockchain is actually another innovation which additionally implies that common blockchain is a restricted measure of accessible capacity to manage applications. The cost of blockchain capacity is similarly high which can make the expenditure related to the use and maintenance of blockchain higher.

Database-related capability, then, is anything but difficult to obtain. They are additionally moderate, and can even manage the costs of contracting the independent enterprise database master.

### **Blockchain vs. Database: Speed and Performance**

The speed of execution is additionally a basic viewpoint which we have to analyse both blockchain and database. Databases are known for quicker execution time and can likewise deal with a huge number of information at some random time.

Blockchain is impressively slower when contrasted with databases. Notwithstanding, it tends to be on the grounds that blockchain is generally new innovation and still needs a great deal of time to develop and coordinate to the guidelines of well-matured advances, for example, databases.

At the point when an exchange did in the blockchain, it does every one of the things that a conventional database will do. Be that as it may, it is backed off in light of conveying more activities including the accompanying.

1. **Signature confirmation:** Blockchain exchange when done are cryptographically marked utilizing cryptographic calculations. This progression is expected to ensure that every exchange is legitimate and is begun from a substantial source. As it is a mind boggling process, it sets aside some effort to do the procedure. Despite the fact that the entire blockchain application is quick, the mark confirmation can bottleneck. In correlation, a brought together database doesn't need to experience the mark check process which makes them similarly quicker.

2. **Consensus components:** As blockchain is decentralized, it depends intensely on accord instrument to approve exchanges on to the blockchain. Additionally, the speed of accord relies upon the sort of agreement strategy utilized. Some accord strategy is quicker than others, however in general, it includes additional time before an exchange can be prepared. Unified databases don't experience the ill effects of this sort of issues as they incorporated in nature. Every exchange is confirmed consequently by the database and can be executed way quicker utilizing a line.

3. **Redundancy:** Blockchain is a finished system where every hub assumes a significant job. To ensure that every hub can take cooperation, every exchange data should be put away and confirmed by every hub.

These three perspectives delayed down the blockchain. This implies databases are relatively quicker with regards to execution.

### **Blockchain vs. Database: Best Use Cases**

Now that we have understood some crucial difference between blockchain and databases, it is now time we learn the best uses cases for both of them.

#### **Database Use Cases:**

The best use case for databases is venture arrangements or systems. The explanation for it is the way the database works and carry dependability to the entire system. Databases are without a doubt easy to use and are as of now bolstered by numerous well-known administration frameworks for engineers and managers. Indeed, even sites with a great many guests depend on databases to serve content. Forbes, for instance, utilizes database related to very good quality frameworks. The versatility is the thing that settles on databases such a decent decision for the undertakings out there. Likewise, frameworks, for example, stock trade that depend on quick tasks must utilize databases for better information stream. Be that as it may, blockchain additionally appears to do extraordinary in big business systems.

The blockchain isn't perfect to store an immense measure of numerical information that should be routinely utilized. Another advantage is the manner by which information is put away in a database. It doesn't need to experience confirmation during the compose or read process. What makes an extraordinary decision on a database is an instrument by which it can be very well practical, especially if there is a need to perform fundamental accounting. To sum it up, the best use cases for databases include the following.

- Applications or systems that use a continuous flow of data.
- Storing confidential information
- Online transaction processing which should be fast
- Apps or systems where data verification is not required.
- Data relational data
- Standalone Apps

### **Blockchain Use Cases:**

Blockchain's purpose is completely different. It is a distributed system that builds up two significant things to its clients, i.e., straightforwardness and trust. The disseminated record is the thing that makes it one of a kind. It can change how an industry functions and upgrade each and every part of it. Things being what they are, what are the best use cases for blockchain? How about we investigate.

Any framework that requires legitimate check can use blockchain. For instance, B2B Business-to-Business exchanges can profit hugely. This incorporates production network, stock administration, and circulation. The key here is straightforwardness as it empowers organizations to pursue each and every development without presenting greater unpredictability. In any case, blockchain doesn't scale that much and can hinder frameworks when taking care of huge scale information records.

As we definitely know, Bitcoin uses blockchain. It empowers anybody to send resource from spot to another without uncovering character. Not just that it likewise guarantees that nobody can do two-fold spending.

Another brilliant use instance of blockchain is permissioned systems. Permissioned systems, for example, casting a ballot can profit by a decentralized approach as well as

carry trust and straightforwardness to the entire democratic framework. Hyperledger is an open source activity that is making structures for associations so they can execute permissioned systems absent a lot of trouble. There are additionally different methods for giving accord which makes blockchain incredibly adaptable to the association's needs. As blockchain is non-social, it isn't perfect for frameworks that depend vigorously on social data.

Blockchain is additionally perfect for computerizing assignments inside a stage. Keen agreements are presented in Ethereum blockchain which gets the capacity to use put away strategies. On the off chance that a specific condition is met, the code is naturally executed. Ethereum blockchain additionally utilizes Proof of Stake (PoS) which is progressively proficient and less power hungry.

### **3.3 Steps to be followed for making Blockchain Voting System:**

The Blockchain voting system could have the following steps:

#### **Step1: Candidate's registration**

Up-and-comer can enroll on the blockchain empowered stage to get the votes during races. For enlistment, competitors need to submit PII (actually recognizable Information), that would be put away on the open blockchain (1).

- The competitor's data is available to each partner engaged with the framework. The put away subtleties on the blockchain could assist voters with knowing about the applicants and their abilities before casting a ballot.

- Once the competitor effectively gets enrolled on the stage, the private key would be produced, empowering contender to check the quantity of votes in their record during races.

#### **Stage 2: Voter's enrollment**

To enroll on the stage, a voter would need to submit PII's and confirmation of their citizenship. Furthermore, all the clients' data put away in the IPFS (3).



- The data presented by the voter would be checked through existing government-endorsed frameworks. On the off chance that the records are checked and seen as right, at that point they are permitted to make their record on the framework.
- After effectively joining on the framework, the private key would be produced and the open key will be saved money on the blockchain in the wake of getting confirmed.

Utilizing the private key, the voter can make choice during races.

- All the data put together by the voter is encoded by the private key. Also, voters can see the up-and-comer's profile to check his abilities before throwing a voting form.
- With no uncertainty, the basic part of majority rules system is the mystery polling form; along these lines, it is fundamental to keep up the namelessness of the voter's vote.

### **Stage 3: Voting on Blockchain**

On the political race day, taking an interest competitors can get the votes in their record on the blockchain casting a ballot stage.

- At the hour of races, each voter needs to login to the stage by utilizing the private key. What's more, in the event that it's legitimate, at that point voter can make the choice to their decision of applicant.
- The voter can encode their vote with the open key and send it to the Arbitration Server, guaranteeing the voter's obscurity.
- Meanwhile, the AR is answerable for sending the voter's vote as the democratic token to the proper hub. Every hub would confirm the exchanges as indicated by the guidelines worked in the Smart Contracts.
- The Smart Contracts would be cross-confirming the votes got with the quantity of voter's casted a ballot altogether against all applicants.

- Casting the voting form on the Blockchain includes sending the democratic token to the up-and-comer's record. At the point when the voter signs in the framework, they have the restricted timeframe to send the vote to the up-and-comer's record. On the off chance that they can't send casts a ballot in the set timespan, the shrewd agreement would devastate the democratic tokens.
- The vote put away on the blockchain is unquestionable, permanent and straightforward.

#### **Stage 4: Verifying the vote**

The confirmation procedure of the democratic relies upon the kind of races. A few decisions take into account momentary outcomes and some don't.

- The democratization process depends on the type of ethnic group. A few decisions look at short-term consequences and some do not.
- If a political race was looking at a temporary outcome, at that time one of the blockchain hub could be freely available. In a blockchain system, voting can include an open key and verify if their voting is checked.
- If the political race coordinators need to leave enough result alone, the voter can only get 2 checks with the discretionary server. Regardless of whether, at the end of a political decision, a voter will have the option to confirm whether their voting is designed or not.
- With blockchain, voters can track their voting and can check in case they find the right candidate record. Unless voter information was not attached to it, democratization history would be saved on the blockchain.

#### **Stage 5: Counting the votes**

Casting a ballot could be straightforward with the blockchain framework as it makes simple to follow and assess casts a ballot in the continuous.

- Each voter can cast a ballot once for the up-and-comer of their decision. What's more, the up-and-comer who has the most elevated number of casting a ballot tokens in their record wins the political decision.
- For voters who swore off democratic, their democratic tokens will be sent to a go without account, guaranteeing their vote doesn't get abused. The checking of the polling forms is so natural and can announce the champ of the political race in the most brief range of time.

### Step 6: Election's results

Using the blockchain voting platform, the election results immediately appear. Pre-defined rules built into smart contracts inform those stakeholders that voting has been discontinued with election results.

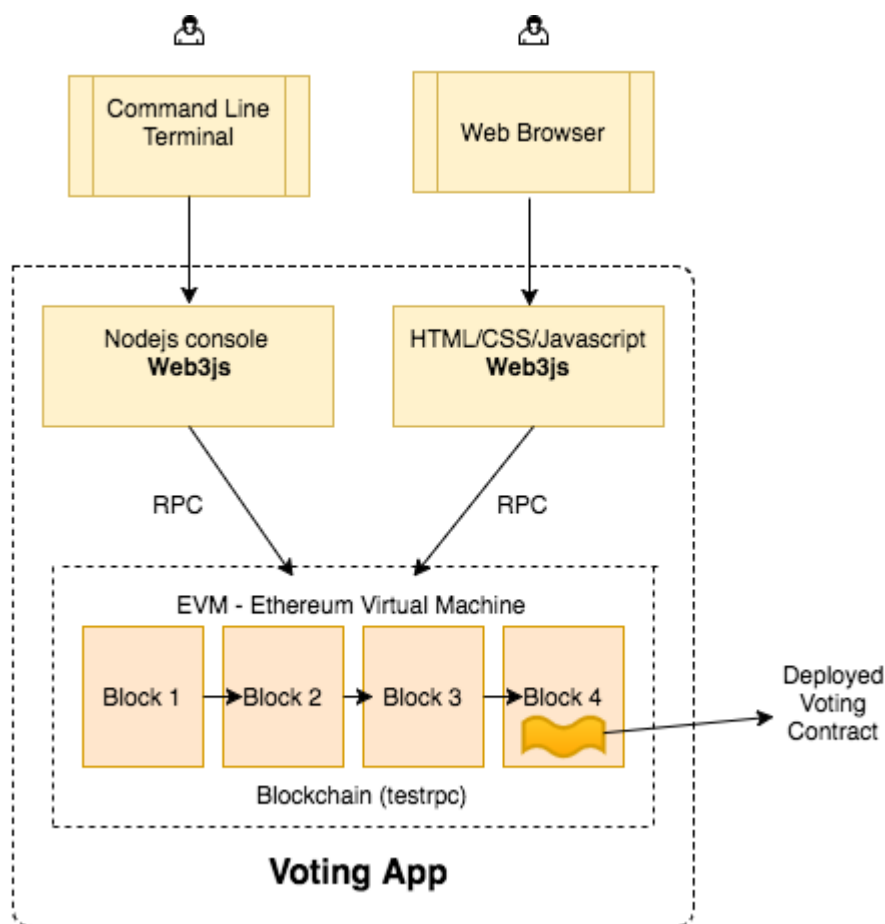


Fig. 3.3. Voting App ERDiagram

## **CHAPTER-4**

### **DEVELOPMENT OF THE VOTING SYSTEM**

#### **Implementation:**

Building simple voting system, a decentralized app on a blockchain. We used an underline and free test technology that will allow us to simulate using a blockchain and also be using a remix as a text editor and simple rpc (remote procedure calls) commands. First, we learned Blockchain concept using remix and rpc commands.

Now for final learning we are using Truffle Suite to create Voting DApp using React application that reads data from the blockchain and displays the data.

#### **What will this app do?**

This will allow to display two possible choices and will allow us to vote for 1 of the choices. For example, we will consider two parties i.e. BJP and Congress. We will keep track of who is voting and we won't allow them to vote again. Each user only gets one

vote. At end we will allow the administrator to end the polling and display the results. The administrator will only be able to start the app and end the polling.

### **How will we do it?**

There will be five main steps to do this. At first, we will write the smart contract. In this we will go to the remix that is free ide that is used to develop the smart contracts. We will write very simple voting system. Second part will be building the interface using JSBin or any other editor that will allow us to write the HTML, CSS and JavaScript code to build the page and install some basic functionality. The third step will be installing testrpc. This will be done using npm system. The fourth step will be connecting the smart contract and interface. We will inject smart contract functionality into the interface build using HTML, CSS and JavaScript. The last step will be running the app locally using the testrpc and web3 technology. We will build smart contract in remix and get the address of the smart contract. Then we will inject it into our webapp and run the webapp.

Now basic features of the final DApp will be Registration of Organizer and Candidate. Then we will create Election. Then we will nominate Candidate for Election. After nomination voting will take place by voter whose first authentication will be done. Then result will be displayed at the scheduled time. Finally, scheduled analysis of the report will be displayed.

### **4.1 Writing the smart contract using Solidity ide remix**

([remix.ethereum.org](https://remix.ethereum.org)).

#### **What do we need in the smart contract?**

Most voting systems have voting and candidate structs.

**Voter struct** represents the single voter. It will keep track of voter name, who they voted for etc. And **Candidate struct** will be the possible candidate for whom the user can vote for. The candidate struct will have name and number of votes they got. After this we will have mappings and arrays to hold lists of these structs to keep the track of who has voted and who our candidates are. We will need constructor to start the new instances of the contract and do a little bit of setup. And also, we will few functions to vote, to get the number of votes and display the results of the polling.

Starting the project using Remix on website remix.ethereum.org. We will start a new smart contract name it as 'simpleVoting.sol'. .sol is an extension used. **sol** file **extension** are files that contain settings and user data that is saved for the Macromedia Flash Player. The **SOL** file **format** is only used by Flash versions 6 and later. After making a smart contract file, we will start to write code. We will use JavaScript VM environment.

1. We are using the latest version of solidity so we will write the **pragma solidity ^0.4.25**; Then we should check that the compiler is set. Then we will write a contract that is simple voting. And then we will write the constructor which we will keep public.

```
pragma solidity ^0.4.25;
```

2. Then we will write the Contract to allow users to cast votes and declare a winner. It gives chance to voters to vote for the candidate they wish to vote for. This contract also allows to declare the winner of the polling.

```
contract Simple Voting {
```

3. Then we will make a Struct to represent the candidate that people can vote for. The struct will have the name of the candidate and the number of votes that the candidate has received.

```
struct Candidate  
  
{  
  
bytes32 name;  
  
uint numberOfVotes;  
  
}
```

4. Then we will make a Struct to represent the person who can Vote for a particular candidate. This struct tells whether the user has voted or not. It also tells the index of the candidate for whom the user has voted for.

```
struct Voter {  
  
    bool voted;  
  
    uint vote;  
  
}
```

5. Then we will make a list. This list will include all the candidates to whom user can vote. The user will choose the candidate to vote from this list.

```
Candidate [] public candidates;
```

6. Then we will make another list. This contains list of users who have voted. This list voters are sorted by their address.

```
mapping(address=>Voter) public votes;
```

7. Then we will write the address for the admin. This administration controls the voting system. For example, we will consider chairperson as an admin.

```
address chairPerson;
```

8. Then we will write a constructor to create a new voting system. This constructor will be of public type.

```
constructor () public {  
  
    chairperson = msg.sender;  
  
    candidates. Push (Candidate ({  
  
        name: 'BJP',  
  
        numberOfVotes: 0  
  
    }));
```

```

    candidates. Push (Candidate ({
    name: 'Congress',
    numberOfVotes: 0
    }));
}

```

9. Then we will write the function to cast a vote. This function takes in the candidate to cast a vote for.

```

function cast Vote (uint candidate Index) public {
    address sender= msg. sender;
    require (! votes[sender]. voted, 'Voter has already voted');

    candidates [candidate Index]. numberOfVotes += 1;
    votes[sender]. voted = true;
    votes[sender]. vote= candidate Index;
}

```

10. Then we will write a function to get the number of votes that a candidate has received. This function takes in the index of the candidate and returns the number of votes they have received.

```

function getNumberOfVotes (uint candidate Index) public view returns
(uint)
{
    return candidates [candidate Index]. numberOfVotes;
}

```



11. This is the last function we will write to get the winner. This function tells who is current in the lead. It returns the name of the candidates with most votes.

```
function get Winner () public view returns (bytes32 winner)  
  
{  
  
uint maxNumberOfVotes;  
  
uint length=candidates. Length;  
  
for (uinti=0; i<length; i++) {  
  
if(candidates[i]. numberOfVotes>maxNumberOfVotes)  
  
{  
  
winner = candidates[i].name;  
  
}  
  
}
```

**Similarly, for the final project we will create three-sol files.**

- 1.Election.sol
- 2.Election1.sol
- 3.Migration.sol

#### **4.2Building the app interface.**

We will setup the initial appearance using HTML, CSS and JavaScript and build the initial behaviour of the app.

We will open the new project in JSBin. We will write HTML code to build the skeleton of the page. Then we will use CSS to style the page. Then we will write JavaScript code for the behaviour.

**Creating Final Project:**

We will install dependencies such as truffle and ganache. Then we will create a new project directory and navigate to it from our terminal. My DApp is called DigiVote-master.

```
mkdir DigiVote-master
```

```
cd DigiVote-master
```

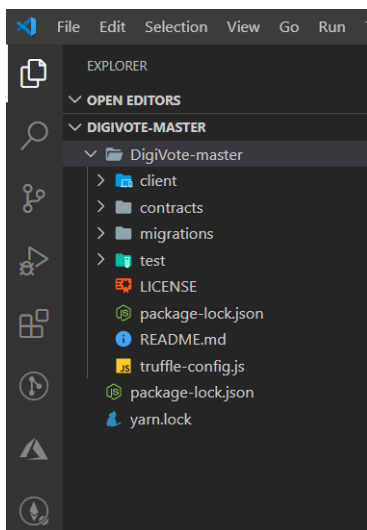
### **Truffle Box:**

We use Truffle Suite to create our DApp. It is a popular framework for developing full-stack decentralized applications on the Ethereum network.

Truffle provides projects called Boxes that are pre-configured to let us focus on functionality rather than fiddling with configuration. We will use React Box which comes with a React front end ready built.

```
truffle unbox react
```

This may take time but once completed we will see folder structure like this in our text editor.



*Figure 4.1: Folder structure*

**client/** contains our front-end React code. We need to delve into this to make changes to our webpage once our contracts have been deployed.

**contract/** is where our Solidity smart contract is stored. We will notice that there are three smart contracts. Migration.sol is used during the migration process.

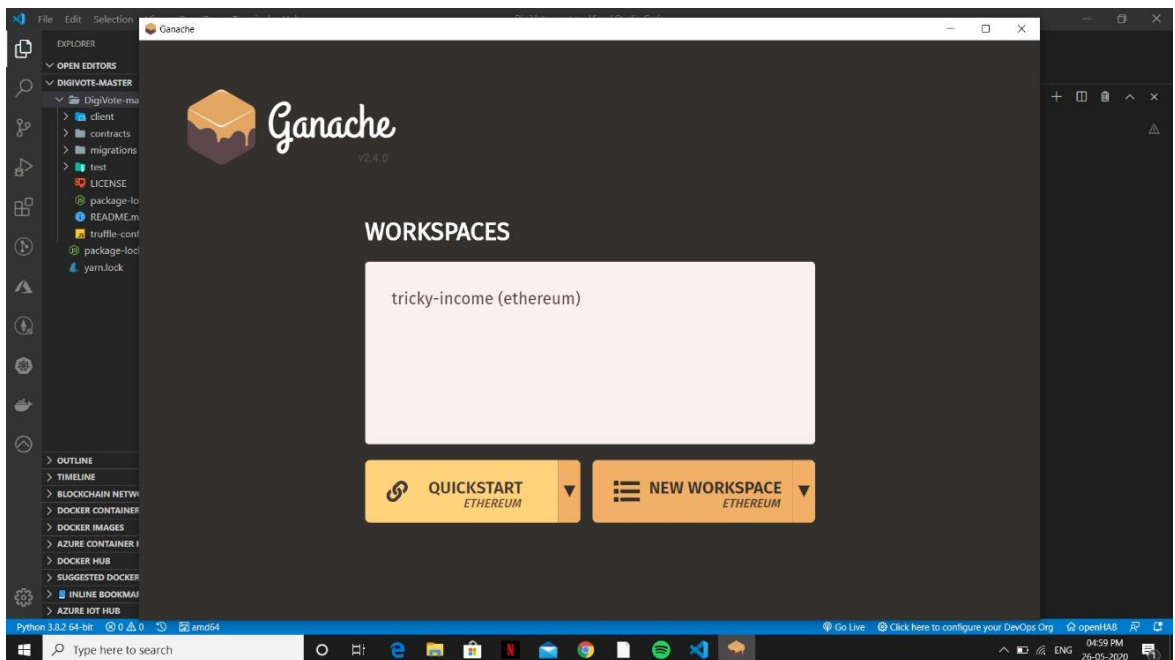
**migrations/** is where migration logic resides.

**test/** is where we test our smart contract to ensure it functions as expected.

**truffle-config.js** -It contains information about networks, compilers, file locations, and other custom configurations for the Truffle framework to know where our things are.

### **Migrating:**

We have to now open Ganache, our local blockchain and make a note of the Network ID and RPC Server information.



*Figure 4.2: Ganache Tool*

We will copy this info into our truffle.config.js file in the project root directory. Make sure our network name is development and not develop.

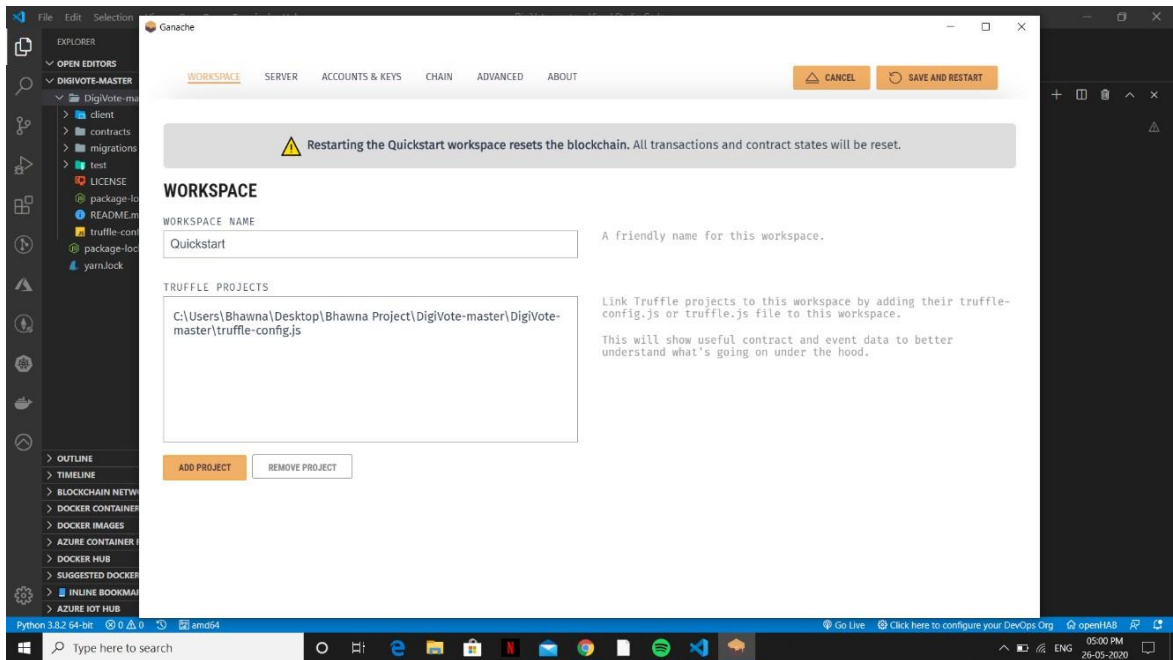


Figure 4.3: Adding Truffle Config file to create Workspace

Now run the following code in your terminal to migrate the smart contract to your Ganache blockchain.

### Truffle migrate

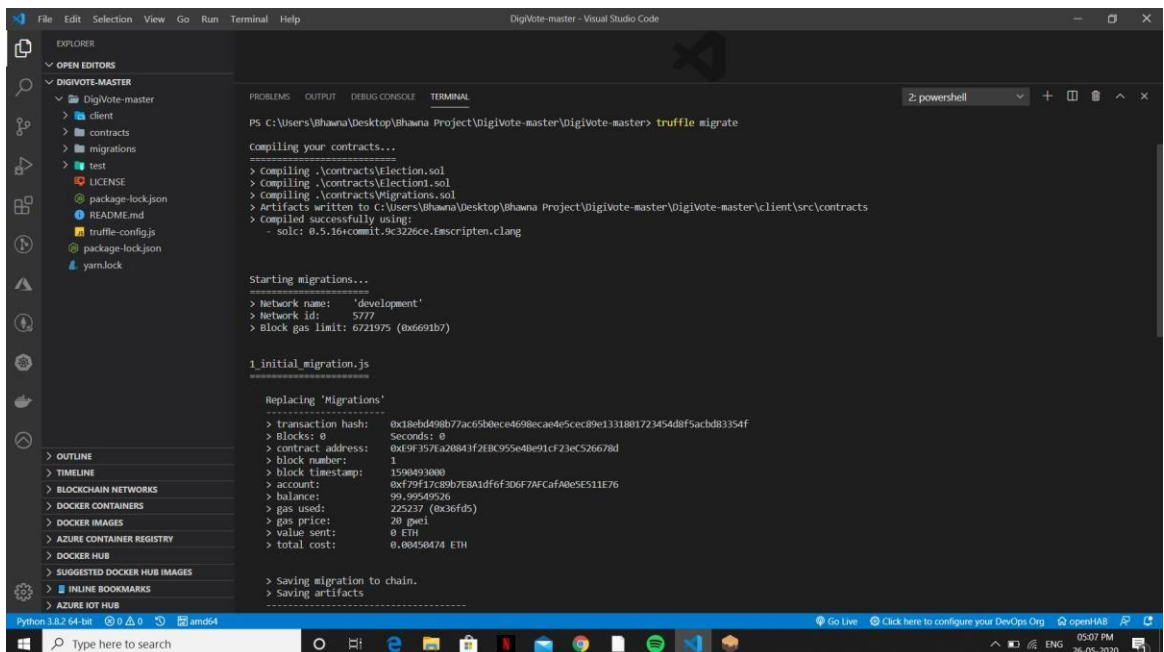


Figure 4.4: Output in the terminal during deploying of the contracts

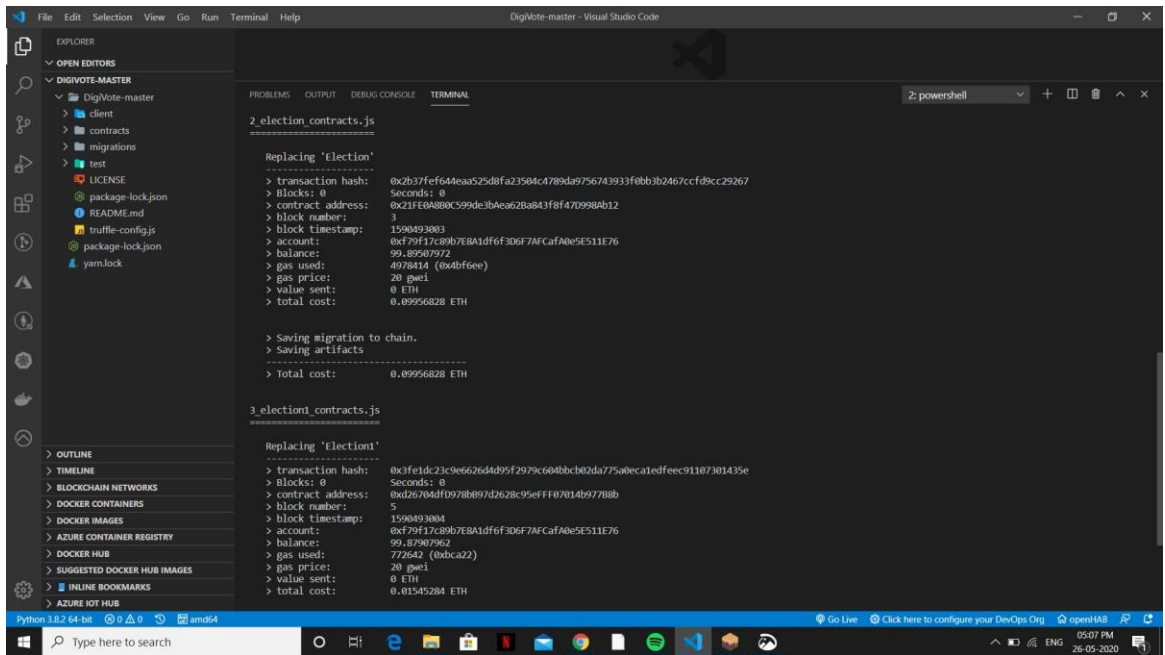


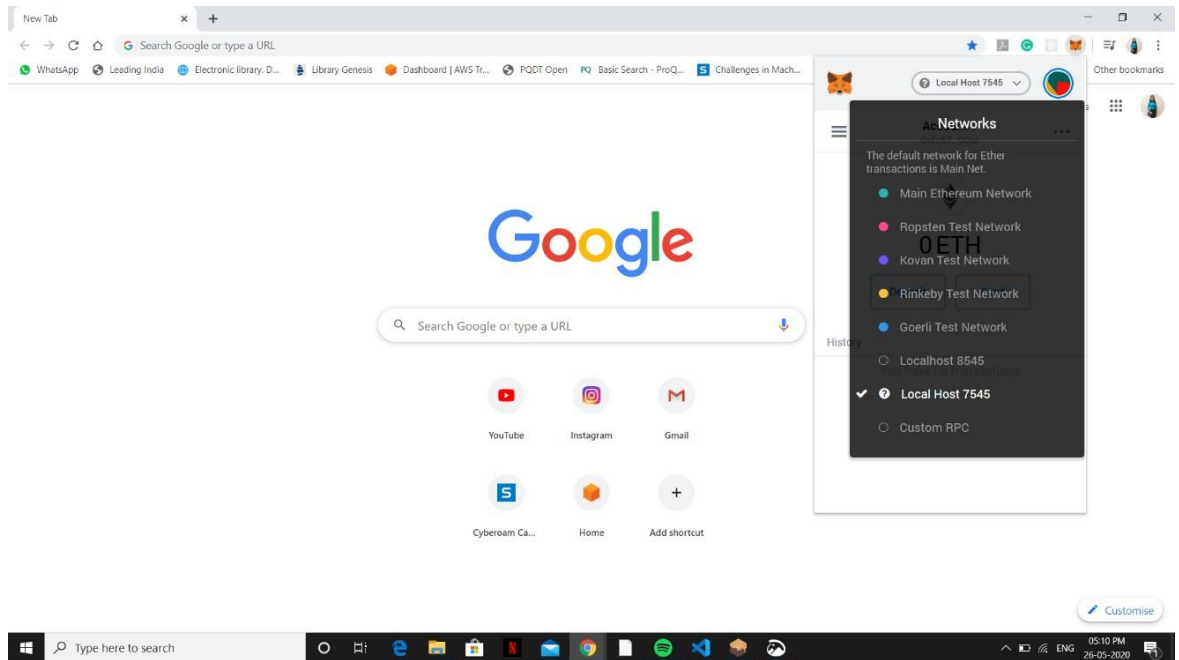
Figure 4.5: Output in the terminal during deploying of the contracts

## React Client:

Before doing any React coding, we need to make sure that our browser can interact with sites that access the blockchain. We do this by using the browser extension called MetaMask.

## MetaMask:

MetaMask is a browser plugin that allows us to make Ethereum transactions through regular websites. We have to install this extension and create the account.



*Figure 4.6: Adding Localhost network to the MetaMask extension*

Next, we click on the MetaMask icon in our browser and log in. There, we need to add a custom RPC so the extension can access your local blockchain. Use the information from Ganache, head back to MetaMask, click Custom RPC, and enter the information. We see it appear in the list of connections with <http://localhost:7545>. Connect to this network by clicking it.

MetaMask creates a wallet address when you create an account, but you can also import other wallet addresses provided you have control of the private keys. This is great for testing because we can use the accounts provided by Ganache to interact with our local blockchain.

Head over to Ganache and copy the private key from the first address in the list. You can display the private key by clicking the key icon on the right side of the row for each account, as shown in Figure.

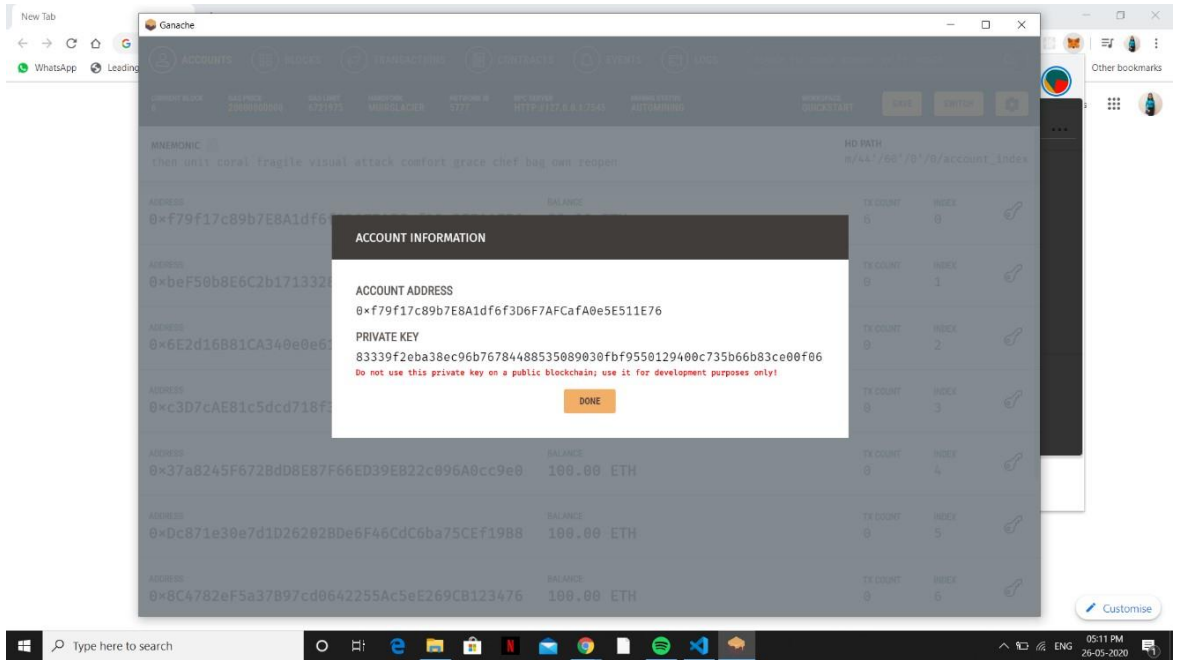


Figure 4.7: Capturing Private Key from Accounts Tab in Ganache Tool

Head back to MetaMask in your browser and open the Accounts panel by clicking on the icon in the top-right corner. Click Import Account, paste the private key in, and click Import. This will add the account to your list of accounts. Select that account. Great! Let's test it out.

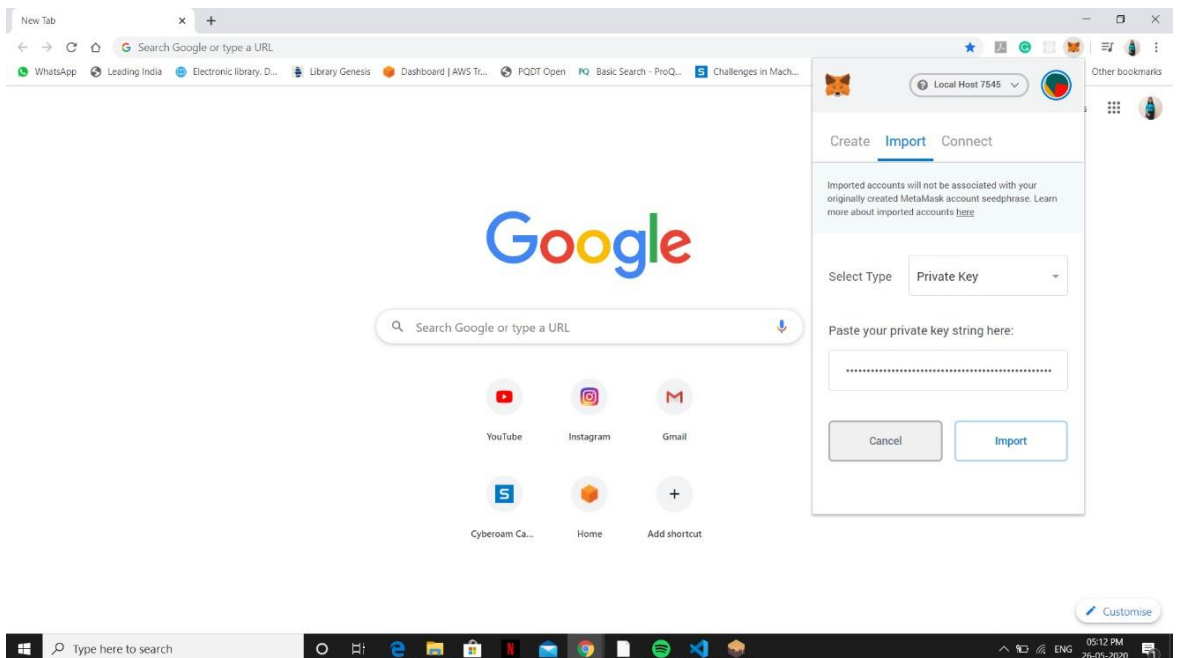
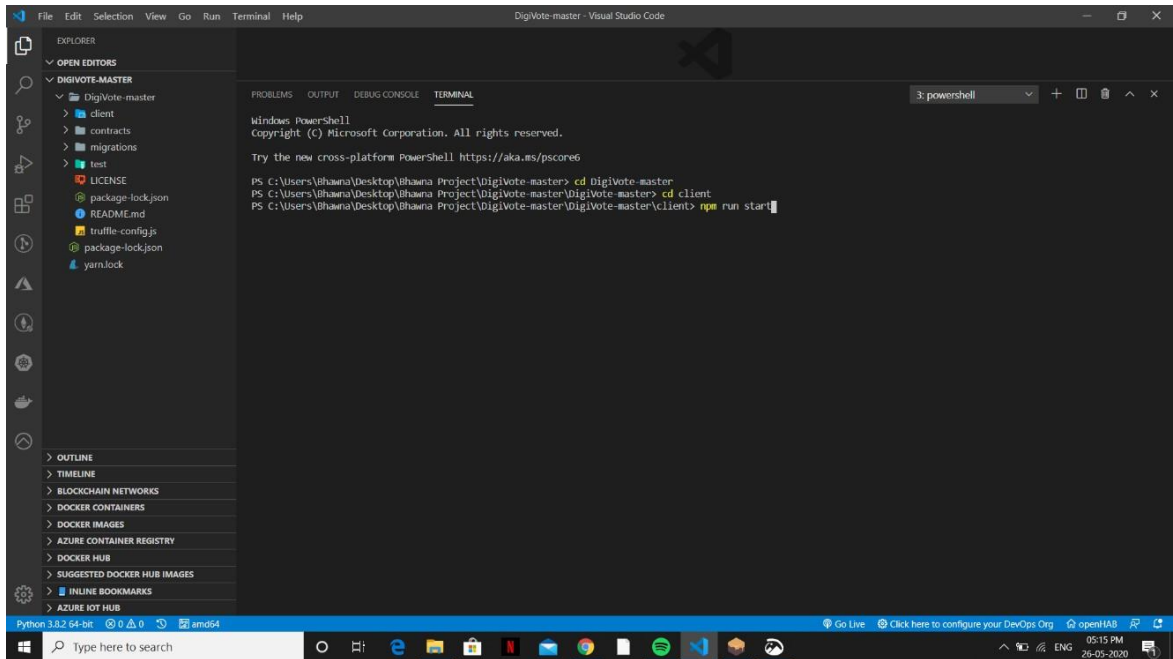


Figure 4.8: Pasting private key string over the MetaMask for connectivity.

## Front end

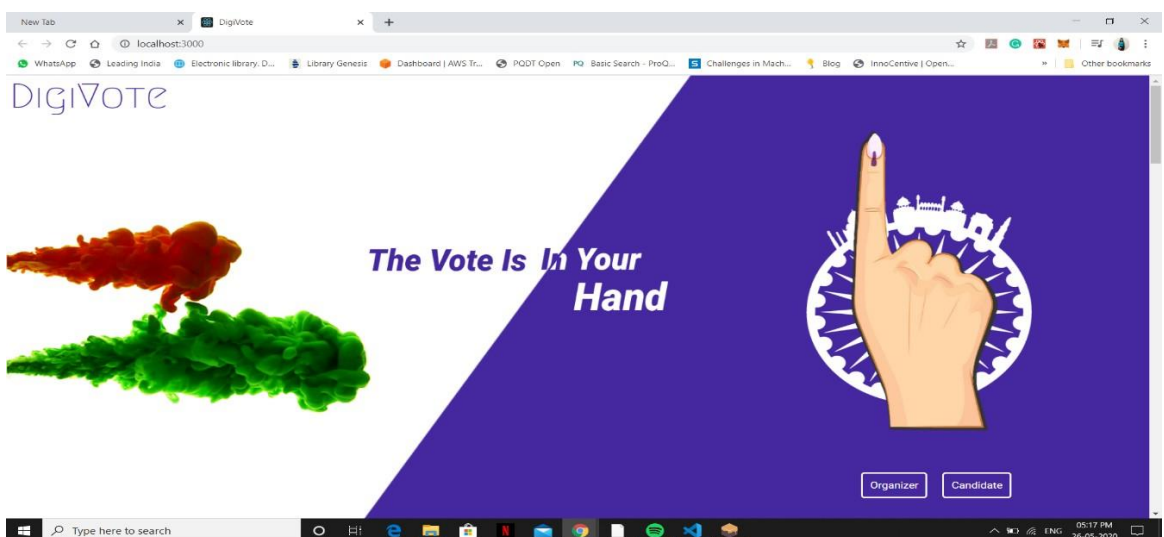
Let's test our React client. As I mentioned earlier, the Truffle Box provides some React boilerplate. In your terminal, navigate into the client/ folder and run the following:

```
npm run start
```



*Figure 4.9 Executing React application through this command*

This should open a new browser tab and attempt to connect your browser to the blockchain. You'll get a notification from the MetaMask extension attempting to connect. Confirm it. This webpage is displayed:



*Figure 4.10 Main Page of DIGIVOTE after execution*



## **Chapter -5**

### **RESULTS AND ANALYSIS**

#### **5.1 Description:**

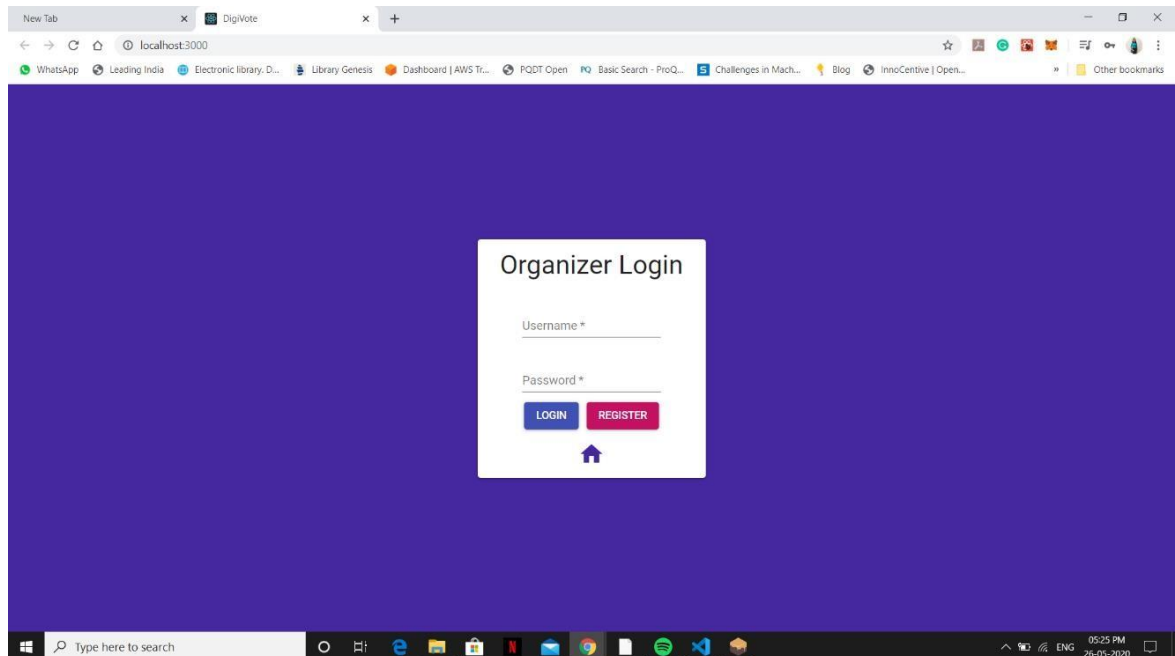
*Exploring the Voting phase*

5. Organizer & Candidate Registration
6. Election Creation
7. Nomination of Candidate for Election.
8. Voting by Voter.
9. Scheduled Result.
10. Scheduled Analysis Report.

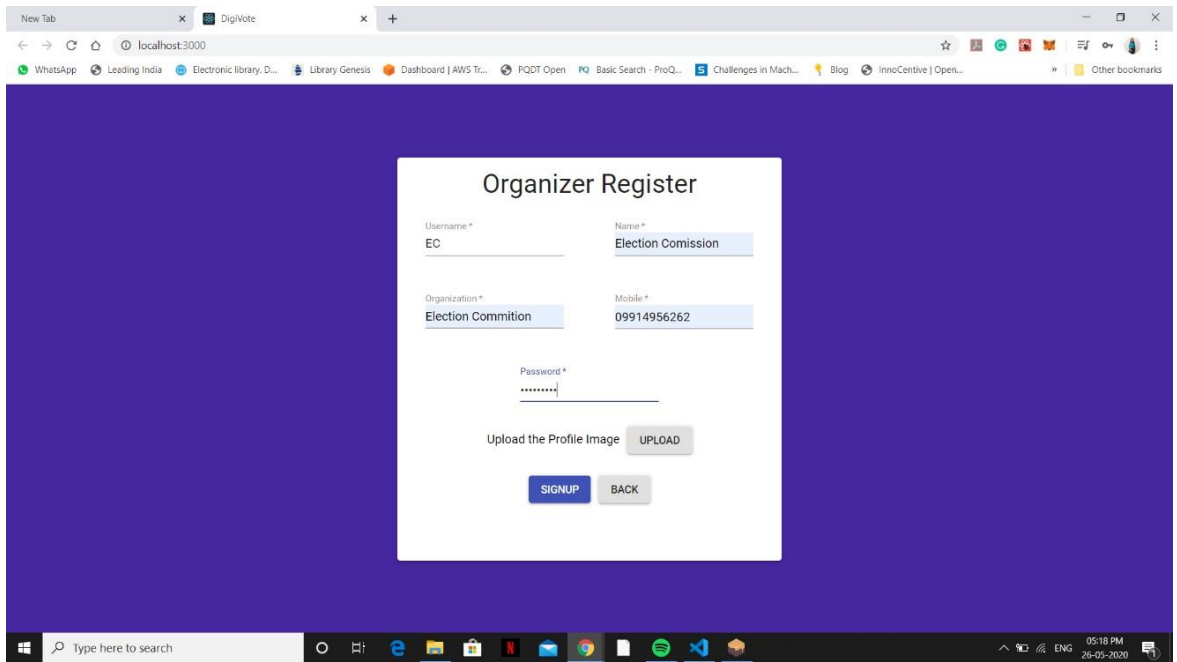
#### **5.2 Outputs:**

##### **1. Organizer and Candidate Registration**

Now on the webpage click on Organizer and register.

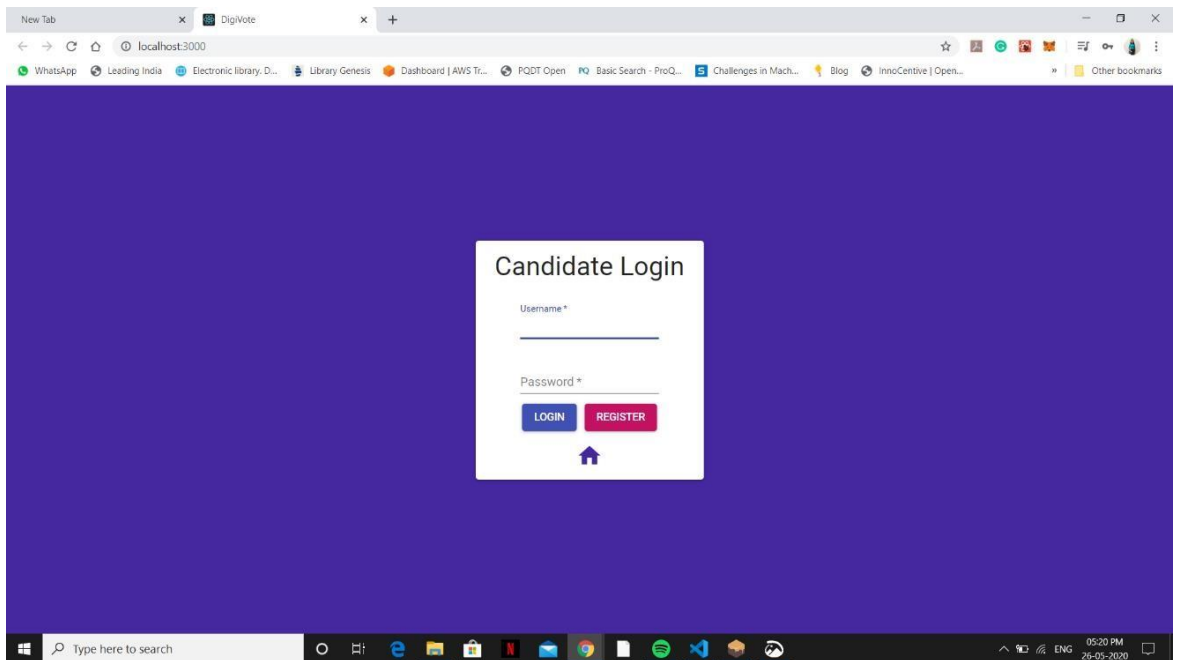


*Figure 5.1 Organizer Login Page*



*Figure 5.2 Organizer Registration Page*

Now click on Home option and then click on Candidate. Now register Candidate.



*Figure 5.3 Candidate Login Page*

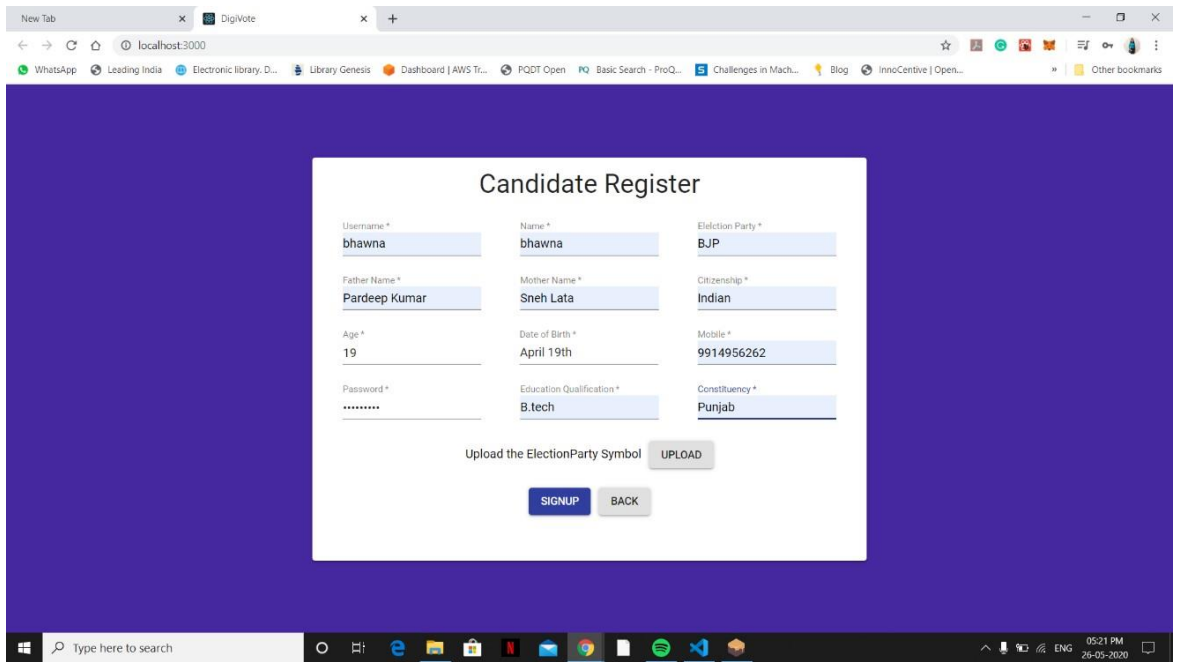


Figure 5.4 Candidate Registration Page

## 2.Election Creation

Now we create Election. We go to Organizer on homepage and login as registered organizer. Then we click on create election.

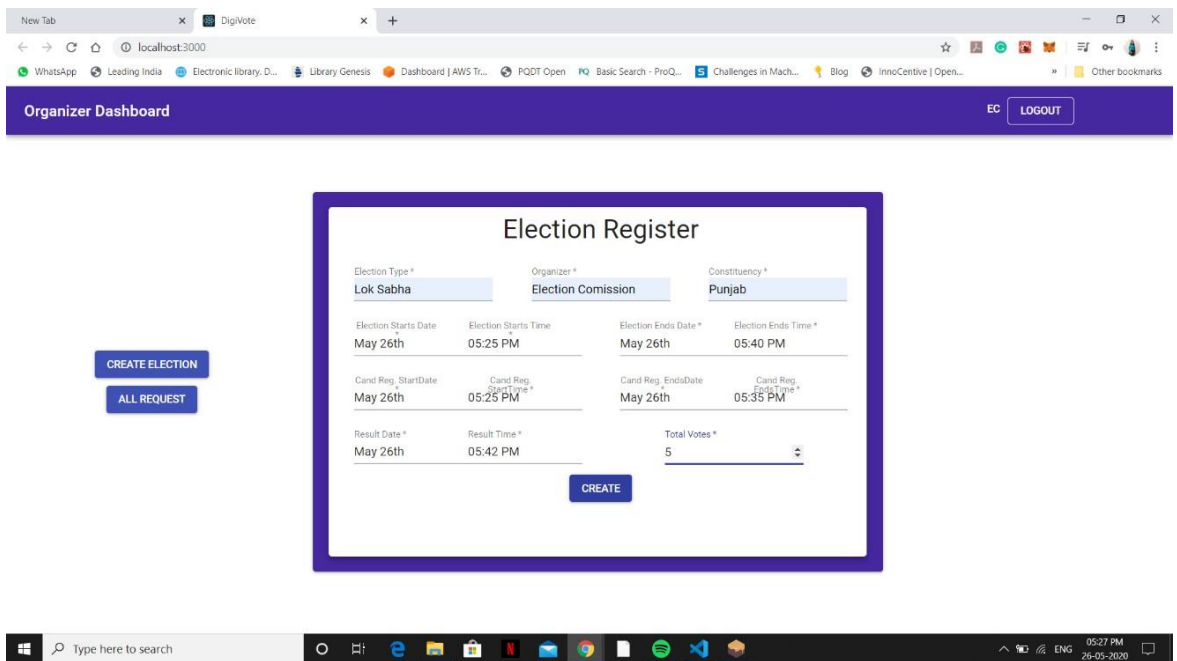


Figure 5.5 Election Registration Page

### 3.Nomination of Candidate for Election

Now we nominate the registered candidates for election. We click on Candidate option on the homepage after logging out of organizer and login as registered candidate.

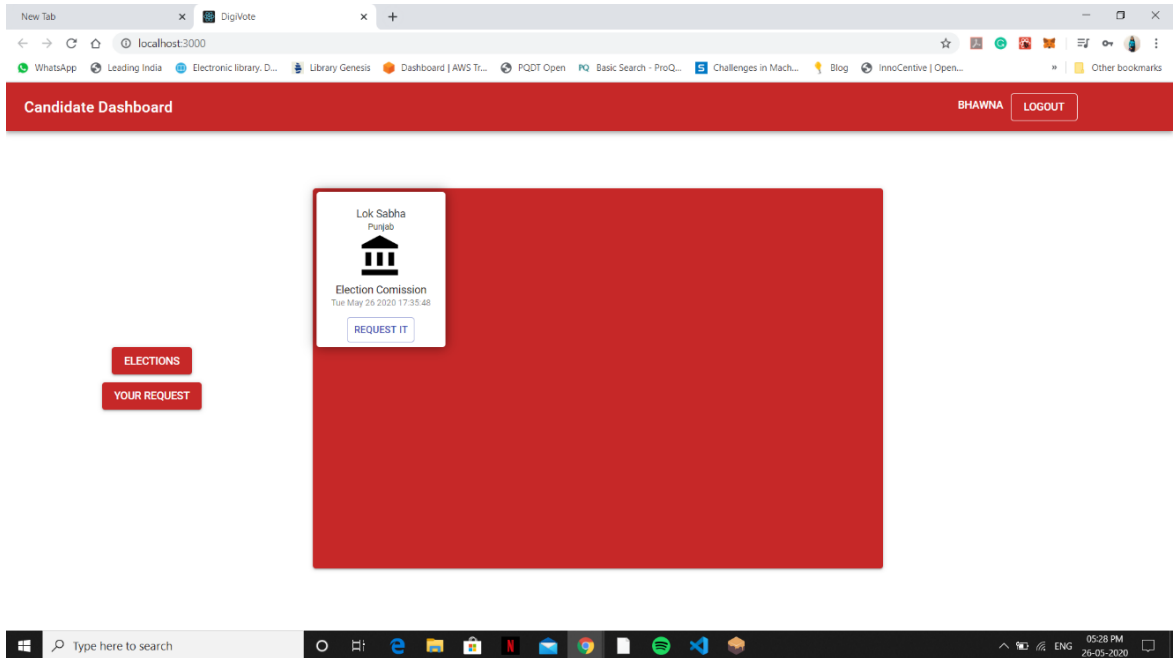


Figure 5.6 Candidate Dashboard

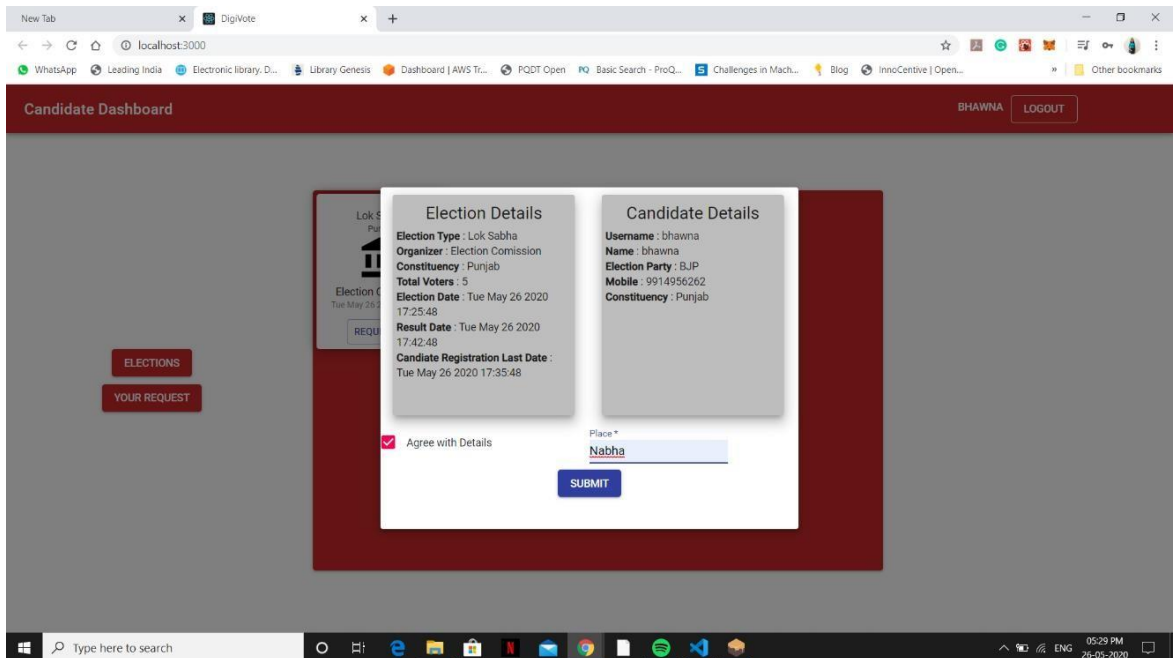


Figure 5.7 Candidate Request

After nominating candidate. Approve the nomination of candidate by going to organizer all requests.

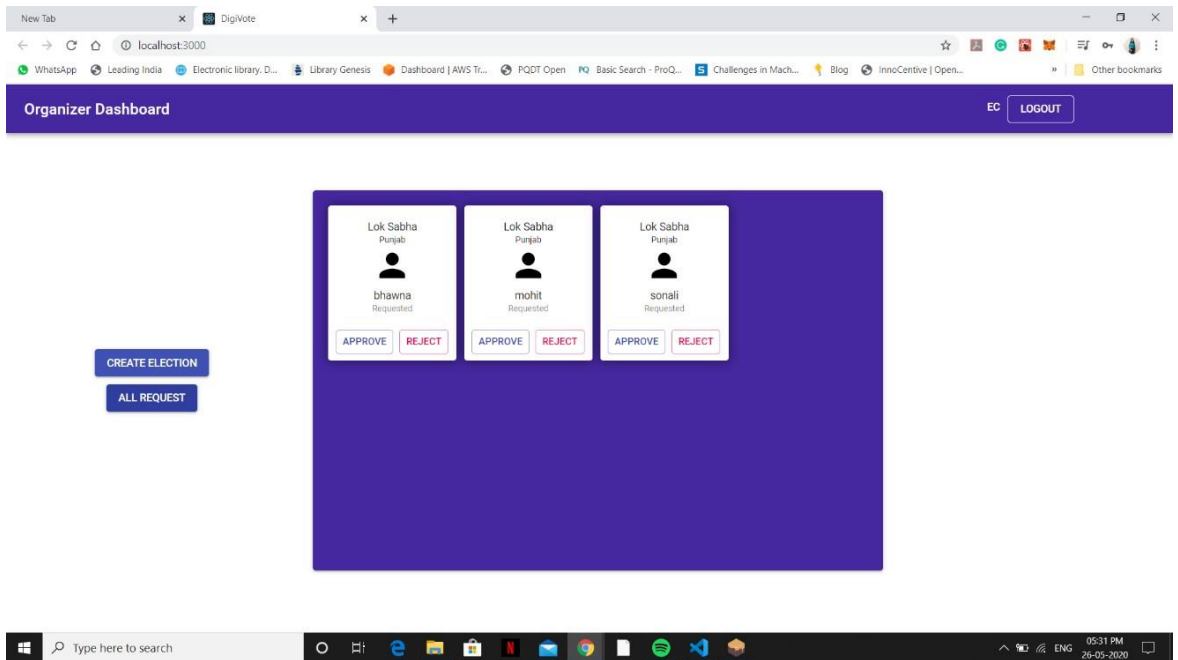


Figure 5.8 Organization Approval Dashboard

### 1. Voting by Voter

Now voting will take place. Click on vote by clicking on reanalysis election option on homepage.

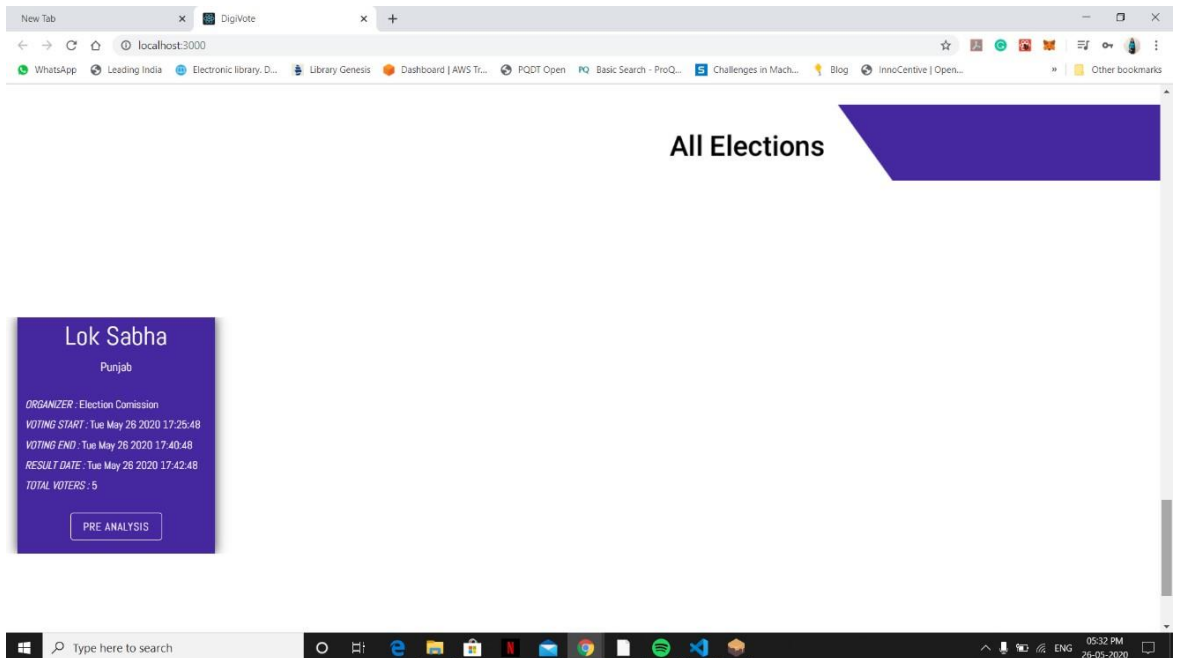


Figure 5.9 Live Elections

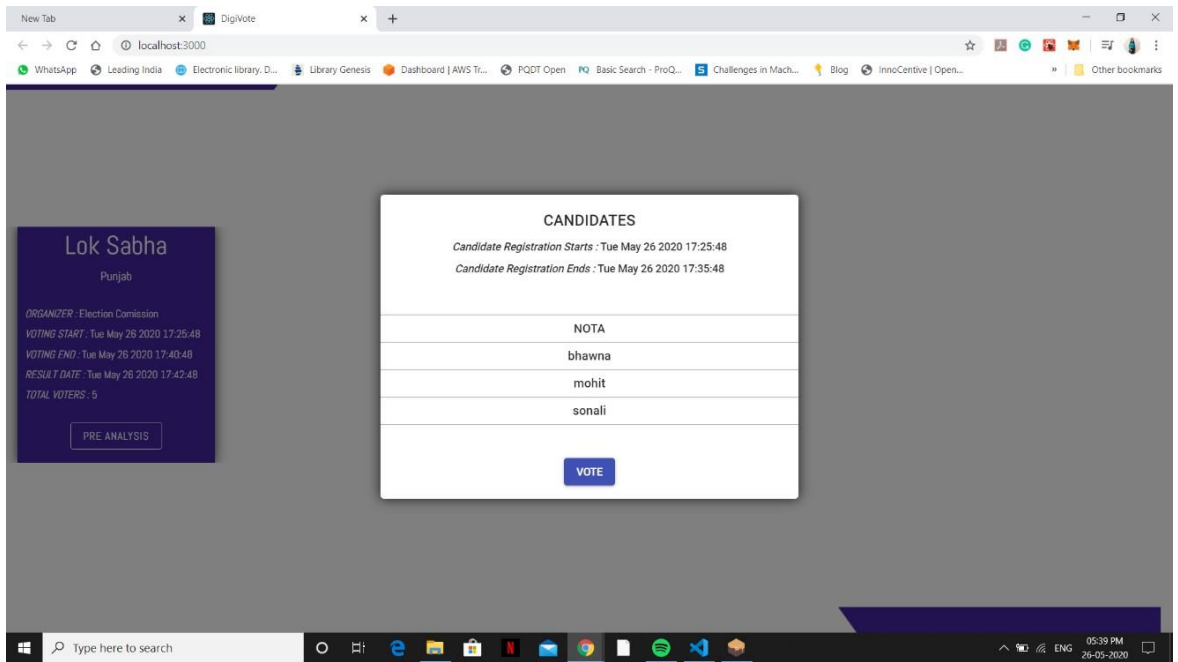


Figure 5.10 Vote candidates

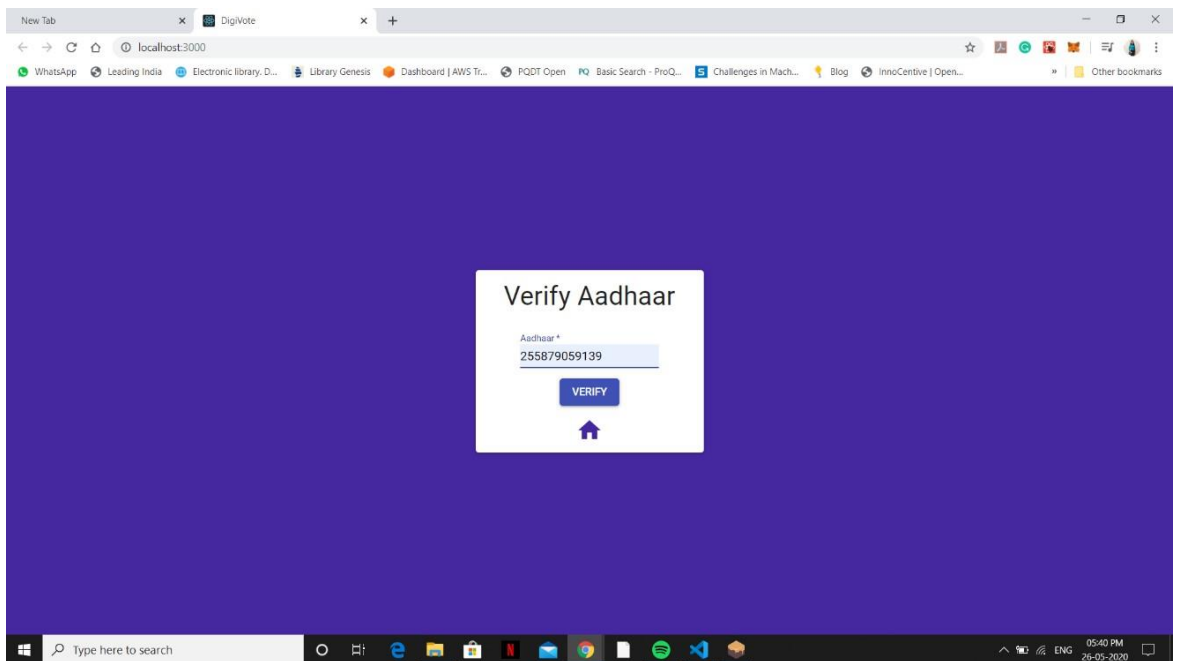


Figure 5.11 Aadhaar Card Verification

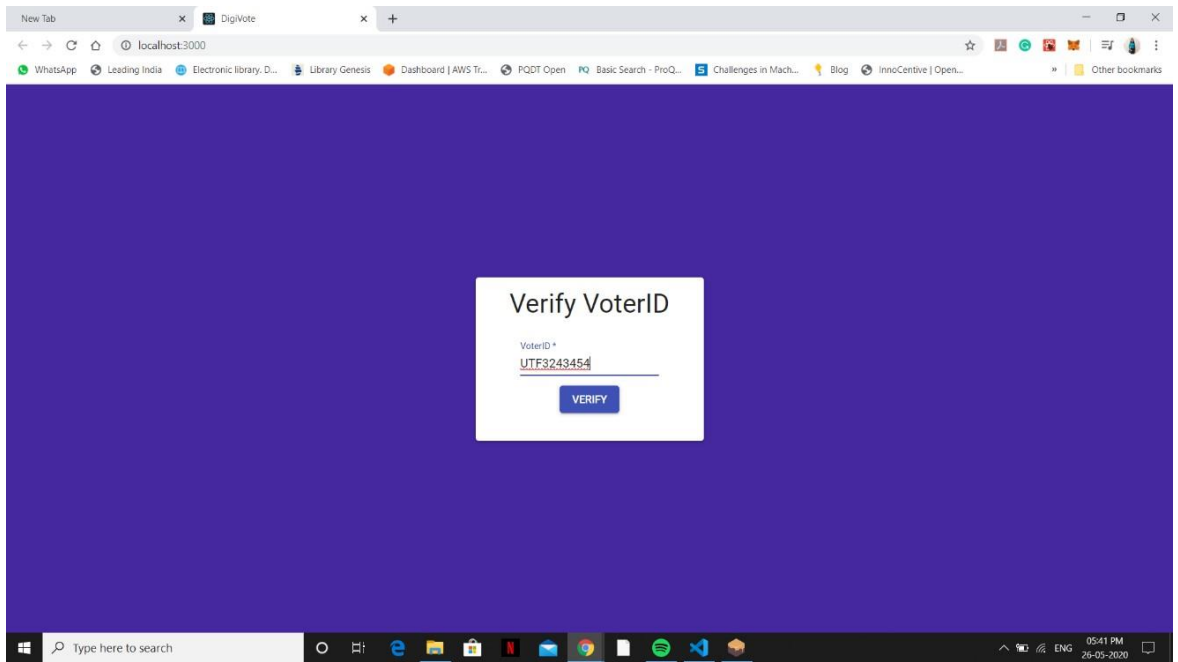


Figure 5.12 Voter Card Verification

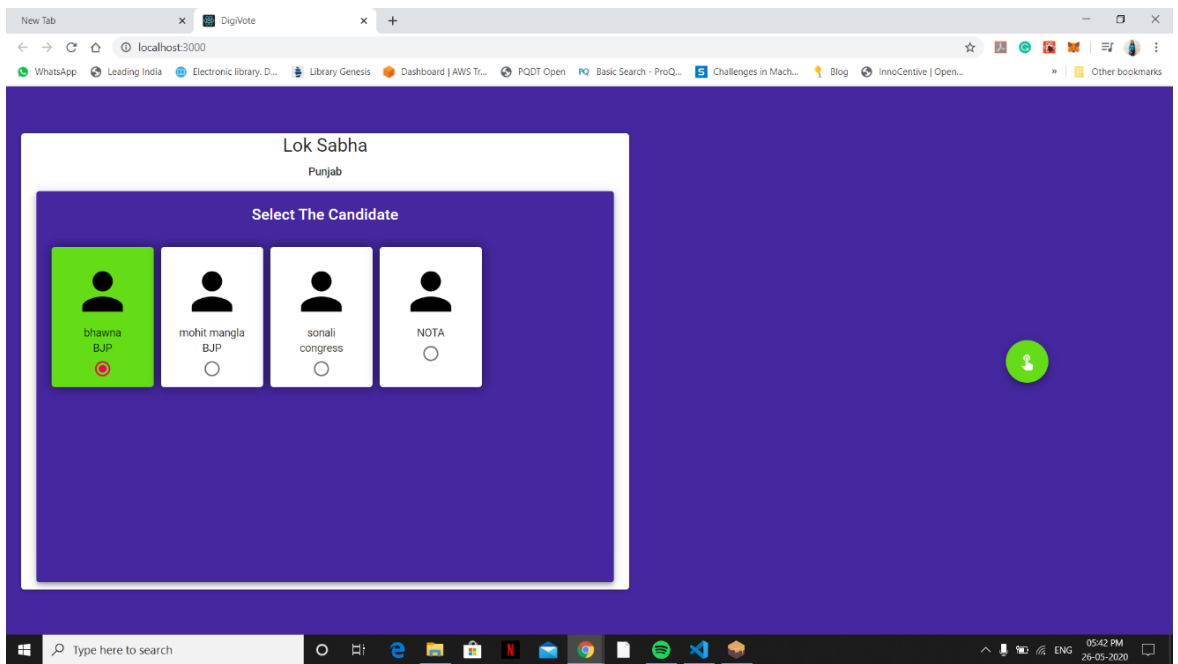


Figure 5.13 Lok Sabha Vote for Candidate

### 5.3 Security Analysis and Legal Issues

In this section we analyse the security of the proposed EVS and the main legal issues.

#### A. Security analysis

1) **DDoS**: To effectively DDoS a disseminated framework, for example, we have proposed, the assailant must DDoS each and every boot hub in the private system. The individual or establishment would be promptly found if that would happen. Every hub is executed with a Byzantine adaptation to internal failure calculation, which helps finding bombed hubs in the framework.

2) **Authentication vulnerability**: Every individual is distinguished and confirmed by the framework by showing an electronic ID from Auðkenni and the comparing 6-digit PIN in the democratic stall. Without supervision, an individual could decide in favour of numerous individuals, if the individual knew about the PIN for each relating electronic ID he has. To additionally address this helplessness sooner rather than later, a biometric output could be presented.

3) **Sybil**: Sybil attack is known against concentrated frameworks, where an individual makes an enormous number of hubs trying to upset system activity by commandeering or dropping messages. Since our proposition is running in a private system no individual has the entrance to make one. Indeed, even the agreement convention that is utilized in our framework is inclined Sybil attack. Private blockchains take care of a large number of the present security issues utilizing solid cryptography highlights and the restricted access to the record, without nullifying the straightforwardness perspective the blockchain innovation offers.

#### B. Legal issues

1) **Remote voting**: Remote races give no pressure obstruction as a result of the non-administered factor in a remote political decision. Remote decisions can consequently not ensure the protection that individuals have when they make their choice in a democratic corner. Relatives or a coercer can look out for your shoulder while you're casting a ballot, which could prompt a misconfigured result. On the off chance that races are facilitated on a site for instance it could undoubtedly be brought somewhere near individuals with great hacking abilities and the mentality to do as such. Individuals could recognize themselves



as someone else and along these lines vote in favor of someone else and even various individuals.

**2) Transparency:** In the present political decision plot, no strategy for straightforwardness can be offered to members of the political race. At the point when an individual spots his voting form in the container at his democratic locale, there is no assurance from the plan that his vote was checked and tallied accurately. Any individual vote can be lost, checked erroneously in view of human mistake or just in light of the fact that the gathering which the voter decided in favor of could be loathed by the person which tallied the vote. This straightforwardness is non-existent in light of the fact that no polling form has data on who made previously mentioned choice. To present straightforwardness during the time spent a political decision would require another law which would permit government authorities to offer the types of assistance which permit such technique for straightforwardness

**3) Voter protection:** In each pen and paper political race conspire, voter's security is a key component. The law prohibits any individual or element to have the option to know from a solitary vote, who gave previously mentioned vote. In the event that such data could be assembled for each vote, such data could then break to the open which would take into consideration posting each and every person who decided in favor of a solitary gathering/applicant. To fulfill the protection of every voter, no individual vote ought to be recognizable back to the voter.

## Chapter-6

### **CONCLUSION**

Adapting e-casting a ballot frameworks to make the open discretionary procedure less expensive, quicker and simpler, is a convincing one in present day society. Making the appointive procedure modest and speedy, standardizes it according to the voters, expels a specific force hindrance between the voter and the chosen authority and squeezes the chosen official. It additionally opens the entryway for a more straightforward type of vote based system, permitting voters to communicate their will on singular bills and suggestions.

In this report, we presented a one of a kind, blockchain-based electronic democratic framework that uses brilliant agreements to empower secure and cost-proficient political race while ensuring voters protection. We have illustrated the frameworks engineering, the plan, and a security investigation of the framework. We have indicated that the blockchain innovation offers an additional opportunity for fair nations to progress from the pen and paper political decision plot, to a more expense and time-productive political decision conspire, while expanding the safety efforts of the todays plan and offer additional opportunities of straightforwardness.

Utilizing an Ethereum private blockchain, it is conceivable to send several exchanges for each second onto the blockchain, using each part of the savvy agreement to facilitate the heap on the blockchain. This online voting system is managing the generation of result of an electoral process held among specific number of parties(candidates). Voter has the right to contribute its vote and check the election result.

Furthermore, the admin and candidate panels' creation are in progress. Admin will have the right to start and end the election.

## **REFERENCES**

[1] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson “BLOCKCHAIN-BASED E-VOTING SYSTEM” School of Computer Science Reykjavik University, Iceland.

[2] Emre Yavuz, Ali Kaan Koç, Umut Can Çabuk, Gökhan Dalkılıç “TOWARDS SECURE E-VOTING USING ETHEREUM BLOCKCHAIN”: 2018 6th International Symposium on Digital Forensic and Security (ISDFS), IEEE.

[3] Teogenes Moura, Alexandre Gomes “BLOCKCHAIN VOTING AND ITS EFFECTS ON ELECTION TRANSPARENCY” Proceedings of the 18th Annual International Conference on Digital Government Research.

[4] Ahmed Ben Ayed “A CONCEPTUALLY SECURE BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEM” School of Computer Science Reykjavik University, Iceland.

## uniino votiny s

---

2

SIHILAREF¥ INDEX

12%

INTERHET SOURCES

2%

PUBLICATIONS

10%

STUDENT PAPERS

---

1

101blockchains.com

Internet Source

7».

2

www.leewayhertz.com

Internet Source

4«

3

Submitted to Northcentral

Student Paper

2%



4

Submitted to The British Goilege

Student Paper

1«



5

Submitted to Asia Pacific University Cottega of  
Technology and Innovation (UCTI)

Student Paper

1%



6

Submitted to Siddaganga Institute of  
Technology

Sludeot Paper

1%

7

www.couraehero.com

1•< i

8

Paras Pant, Ruchlka Bathla, Sunil Kumar Khatri.  
“A Model to Implement and Secure Online

1«

---

8 Paras Pant, Ruchika Bathla, Sunil Kumar Khatri. "A Model to Implement and Secure Online Documentation using Blockchain", 2019 4th 1%

International Conference on Information Systems and Computer Networks (ISCON), 2019

Publication

---

9 "Blockchain Based E-Voting System", International Journal of Engineering and Advanced Technology, 2019 1%

Publication

---

10 Submitted to University of East London <1%

Student Paper

---

11 Submitted to International University of Malaya-Wales <1%

Student Paper

---

12 Submitted to Higher Education Commission Pakistan <1%

Student Paper

---

13 file.org <1%

Internet Source

---

14 "Iot Based Smart Wallet Security and Fake Currency Detection System", International Journal of Innovative Technology and Exploring <1%

**JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT**

**PLAGIARISM VERIFICATION REPORT**

Date: 16-07-2020

Type of Document (Tick):  PhD Thesis  M.Tech Dissertation/ Report  B.Tech Project Report  Paper

Name: Bhawna Department: CSE/IT Enrolment No 161476

Contact No. 9914956262 E-mail. Bhawnamangla98@gmail.com

Name of the Supervisor: Mr. Prateek Thakral

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): ONLINE VOTING SYSTEM DAPP USING BLOCKCHAIN CONCEP

**UNDERTAKING**

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/ revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

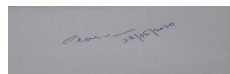
**Complete Thesis/Report Pages Detail:**

- Total No. of Pages = **61**
- Total No. of Preliminary pages = **49**
- Total No. of pages accommodate bibliography/references = **12**

*Bhawna*  
(Signature of Student)

**FOR DEPARTMENT USE**

We have checked the thesis/report as per norms and found **Similarity Index** at ...21.....(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.



(Signature of Guide/Supervisor)

Signature of HOD

**FOR LRC USE**

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
	<ul style="list-style-type: none"> <li>• All Preliminary Pages</li> <li>• Bibliography/Images/Quotes</li> <li>• 14 Words String</li> </ul>		Word Counts	
<b>Report Generated on</b>			Character Counts	
		<b>Submission ID</b>	Total Pages Scanned	
			File Size	

Checked by  
Name & Signature

Librarian

**Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at [plagcheck.juit@gmail.com](mailto:plagcheck.juit@gmail.com)**

**JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT**

**PLAGIARISM VERIFICATION REPORT**

Date: 16-07-2020

Type of Document (Tick):  PhD Thesis  M.Tech Dissertation/ Report  B.Tech Project Report  Paper

Name: Sonali Sehgal Department: CSE/IT Enrolment No 161235

Contact No. 8894256016 E-mail. sehgalsonali.ss@gmail.com

Name of the Supervisor: Mr. Prateek Thakral

Title of the Thesis/Dissertation/Project Report/Paper (In Capital letters): \_\_\_\_\_  
ONLINE VOTING SYSTEM DAPP USING BLOCKCHAIN CONCEP

**UNDERTAKING**

I undertake that I am aware of the plagiarism related norms/ regulations, if I found guilty of any plagiarism and copyright violations in the above thesis/report even after award of degree, the University reserves the rights to withdraw/ revoke my degree/report. Kindly allow me to avail Plagiarism verification report for the document mentioned above.

**Complete Thesis/Report Pages Detail:**

- Total No. of Pages = **61**
- Total No. of Preliminary pages = **49**
- Total No. of pages accommodate bibliography/references = **12**



(Signature of Student)

**FOR DEPARTMENT USE**

We have checked the thesis/report as per norms and found **Similarity Index** at 21.....(%). Therefore, we are forwarding the complete thesis/report for final plagiarism check. The plagiarism verification report may be handed over to the candidate.



(Signature of Guide/Supervisor)

Signature of HOD

**FOR LRC USE**

The above document was scanned for plagiarism check. The outcome of the same is reported below:

Copy Received on	Excluded	Similarity Index (%)	Generated Plagiarism Report Details (Title, Abstract & Chapters)	
	<ul style="list-style-type: none"> <li>• All Preliminary Pages</li> <li>• Bibliography/Images/Quotes</li> <li>• 14 Words String</li> </ul>		Word Counts	
<b>Report Generated on</b>			Character Counts	
		<b>Submission ID</b>	Total Pages Scanned	
			File Size	

Checked by  
Name & Signature

Librarian

.....

**Please send your complete thesis/report in (PDF) with Title Page, Abstract and Chapters in (Word File) through the supervisor at [plagcheck.juit@gmail.com](mailto:plagcheck.juit@gmail.com)**